

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Kenji OHKUMA, et al.

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HEREWITH

FOR: ENCRYPTION APPARATUS AND METHOD, AND DECRYPTION APPARATUS AND METHOD BASED
ON BLOCK ENCRYPTION



REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2000-198478	June 30, 2000

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
(B) Application Serial No.(s)
 - ☐ are submitted herewith
 - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak

Registration No. 24,913
C. Irvin McClelland

Registration Number 21,124



22850

日 本 国 特 許 庁
JAPAN PATENT OFFICE

JC903 U.S. PTO
09/893785
09/893785

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出 願 年 月 日
Date of Application:

2000年 6月30日

出 願 番 号
Application Number:

特願2000-198478

出 願 人
Applicant(s):

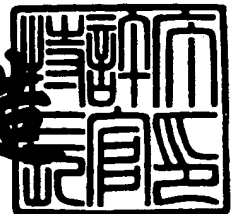
株式会社東芝

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 5月31日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-305093

【書類名】 特許願

【整理番号】 A000003588

【提出日】 平成12年 6月30日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00

【発明の名称】 暗号化装置及び暗号化方法、復号装置及び復号方法並び
に記録媒体

【請求項の数】 18

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研
 究開発センター内

 【氏名】 大熊 建司

【発明者】

 【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中事業所内

 【氏名】 佐野 文彦

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研
 究開発センター内

 【氏名】 村谷 博文

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研
 究開発センター内

 【氏名】 川村 信一

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100058479

 【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】	明細書	1
【物件名】	図面	1
【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 暗号化装置及び暗号化方法、復号装置及び復号方法並びに記録媒体

【特許請求の範囲】

【請求項 1】

ブロック暗号方式による暗号化装置であって、

ブロックデータに対してそれを複数に分割した部分データごとに局所的な拡散を行う機能を含む第 1 の処理手段と、

前段の前記第 1 の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第 1 の処理手段へ入力する機能を含む第 2 の処理手段とを備え、

前記第 2 の処理手段は、前段の前記第 1 の処理手段に対する入力ブロックデータにおける少なくとも 1 つの特定ビットの状態を、後段の前記第 1 の処理手段に対する入力ブロックデータにおける少なくとも 1 つの特定ビットへ、複数の演算経路を辿って波及させるための手段を含むものであることを特徴とする暗号化装置。

【請求項 2】

前記特定ビットは、各々の前記入力部分データに少なくとも 1 つずつ存在することを特徴とする請求項 1 に記載の暗号化装置。

【請求項 3】

前記第 2 の処理手段は、前段の前記第 1 の処理手段に対する入力ブロックデータから選択した 1 ビットと、後段の前記第 1 の処理手段に対する入力ブロックデータから選択した 1 ビットとからなる全ての組み合わせ又はそのうちで所定の条件を満たす複数の組み合わせの各々について、前段側における当該 1 ビットの状態を、後段側における当該 1 ビットへ、複数の演算経路を辿って波及させるための手段を含むものであることを特徴とする請求項 1 に記載の暗号化装置。

【請求項 4】

ブロック暗号方式による暗号化装置であって、

ブロックデータを複数に分割した各分割部分データに対してそれぞれ非線形変

換処理を施す並列させた複数の第 1 の非線形変換処理手段の一群と、ブロックデータのブロック幅にわたる線形拡散処理を施す第 1 の線形拡散処理手段とを備え

前記第 1 の非線形変換処理手段は、前記部分データのデータ幅をさらに複数の分割した各再分割部分データに対してそれぞれ非線形変換処理を施す並列させた複数の第 2 の非線形変換処理手段の一群と、前記部分データのデータ幅にわたる線形拡散処理を施す第 2 の線形拡散処理手段とを含むものであり、

前記第 1 の線形拡散処理手段は、前段の複数の第 1 の非線形変換処理手段の各々の最終段に並列させた複数の第 2 の非線形変換処理手段の各々から出力される全再分割部分データからなるブロックデータに線形拡散処理を施して後段の複数の第 1 の非線形変換処理手段の各々の初段に並列させた複数の第 2 の非線形変換処理手段の一群の各々へ各再分割部分データとして入力するものであるとともに、後段の複数の第 1 の非線形変換処理手段の初段の複数の第 2 の非線形変換処理手段への入力となる複数の再分割部分データのうちの少なくとも 1 つを、前段のいずれか同一の第 1 の非線形変換処理手段の最終段の複数の第 2 の非線形変換処理手段から出力される複数の再分割部分データのうちの少なくとも 2 つに基づいて求めることを特徴とする暗号化装置。

【請求項 5】

前記第 1 の線形拡散処理手段は、後段の全第 1 の非線形変換処理手段の各々について、当該後段の第 1 の非線形変換処理手段の初段の複数の第 2 の非線形変換処理手段への入力となる複数の再分割部分データのうちの少なくとも 1 つを、前段の各第 1 の非線形変換処理手段ごとにその最終段の複数の第 2 の非線形変換処理手段から出力される複数の再分割部分データのうちから少なくとも 2 つずつ選択された再分割部分データ群に基づいて求めることを特徴とする請求項 4 に記載の暗号化装置。

【請求項 6】

前記第 1 の線形拡散処理手段は、後段の各第 1 の非線形変換処理手段の初段の各第 2 の非線形変換処理手段への入力となる各再分割部分データを、それぞれ、前段の各第 1 の非線形変換処理手段ごとにその最終段の複数の第 2 の非線形変換

処理手段から出力される複数の再分割部分データのうちから少なくとも2つずつ選択された再分割部分データ群に基づいて求めることを特徴とする請求項5に記載の暗号化装置。

【請求項7】

前記分割部分データはすべて同一ビット長であるとともに、前記再分割部分データはすべて同一ビット長であり、

前記第1の線形拡散処理手段は、各々の前記再分割部分データから相対応する1ビットずつを取りだしたビット群に対して施す線形拡散処理を、該1ビットを取り出す位置を排他的に変えたものについてそれぞれ行うことによって、ブロックデータのブロック幅にわたる線形拡散処理を行うものであることを特徴とする請求項5または6に記載の暗号化装置。

【請求項8】

前記ブロックデータは128ビットであり、前記分割部分データは32ビットであり、前記再分割部分データは8ビットであり、

前記第1の線形拡散処理手段は、16個の前記再分割部分データの各々から同一位置の1ビットずつを取りだして得た16ビットデータに対して施す線形拡散処理を、該1ビットを取り出す位置を排他的に変えた8つの16ビットデータのそれぞれについて行うものであることを特徴とする請求項7に記載の暗号化装置。

【請求項9】

前記第1の線形拡散処理手段は、実回路によって実装されたものであることを特徴とする請求項5ないし8のいずれか1項に記載の暗号化装置。

【請求項10】

前記第1の線形拡散処理手段の入力側のビットと出力側のビットとの間の結合関係は、ガロア体の乗算に基づいて決定されたものであることを特徴とする請求項9に記載の暗号化装置。

【請求項11】

前記第1の線形拡散処理手段は、ソフトウェアを実行することによって実現されるものであることを特徴とする請求項5ないし8のいずれか1項に記載の暗号

化装置。

【請求項 1 2】

共通鍵ブロック暗号方式による暗号化装置であって、

初段では入力された 1 2 8 ビットの平文ブロックデータを、2 段目以降では前段での処理が施された 1 2 8 ビットのブロックデータを入力とし、該ブロックデータを 4 分割した 4 組の 3 2 ビット・データに対してそれぞれ局所的な線形拡散処理および非線形変換処理を施し出力する 4 つの第 1 の非線形変換処理部と、これら 4 つの第 1 の非線形変換処理部からそれぞれ出力された 4 組の 3 2 ビット・データを連結した 1 2 8 ビットのブロックデータに対して最大距離分離行列を用いて線形拡散処理を施し次段へ出力する第 1 の拡散処理部とを、1 段分の段構成として、該段構成を所定段数分接続し、

最後の前記第 1 の拡散処理部の後段に、この第 1 の拡散処理部から出力される 1 2 8 ビットのブロックデータを入力とする前記 4 つの第 1 の非線形変換処理部を接続し、

この 4 つの第 1 の非線形変換処理部の後段に、これら 4 つの第 1 の非線形変換処理部からそれぞれ出力された 4 組の 3 2 ビット・データを連結した 1 2 8 ビットのブロックデータに対して 1 2 8 ビットの鍵データを加算して 1 2 8 ビットの暗号化されたブロックデータとして出力する第 1 の鍵加算部を接続して構成されるとともに、

前記第 1 の非線形変換処理部の各々は、与えられた 1 組の前記 3 2 ビット・データをさらに 4 分割した 4 組の 8 ビット・データに対してそれぞれ 8 ビットの鍵データを加算する 4 つの第 2 の鍵加算部と、各第 2 の鍵加算部の出力に対してそれぞれ 8 ビットの入出力変換表を用いて非線形変換を行う 4 つの第 2 の非線形変換処理部と、これら 4 つの第 2 の非線形変換処理部からそれぞれ出力された 4 組の 8 ビット・データを連結した 3 2 ビット・データに対して最大距離分離行列を用いて線形拡散処理を施す第 2 の拡散処理部と、この第 2 の拡散処理部の後段にさらに接続された 4 組の前記第 2 の鍵加算部および第 2 の非線形変換処理部とを含むものであり、

前記第 1 の拡散処理部の各々は、前段の 1 つの第 1 の非線形変換処理部の 4 つ

の第2の非線形変換処理部からそれぞれ出力される8ビットのうちの相対応する1ビットを一纏めにした4ビットを行列演算における入力側の1つの要素とするとともに、後段の1つの第1の非線形変換処理部の4つの第2の非線形変換処理部へそれぞれ入力される8ビットのうちの相対応する1ビットを一纏めにした4ビットを行列演算における出力側の1つの要素として、 2^4 のガロア体の乗算に基づいた4行4列の行列演算またはこれと等価な回路によって線形拡散処理を行う16ビット拡散手段を、該前段及び後段の第2の非線形変換処理部についての該8ビットのうちの各ビットに対応して有し、

1つの前記16ビット拡散手段における前記 2^4 のガロア体の乗算に基づいた4行4列の行列演算またはこれと等価な回路では、前段の4つの第1の非線形変換処理手段の最終段における合計16の第2の非線形変換処理手段からの出力となる任意の1ビットと、後段の4つの第1の非線形変換処理手段の初段における合計16の第2の非線形変換処理手段へ入力となる任意の1ビットとのすべての組み合わせにおいて、前段側における当該1ビットの状態を、後段側における当該1ビットへ、複数の演算経路を辿って波及させるための手段を含むものであることを特徴とする暗号化装置。

【請求項13】

共通鍵ブロック暗号方式による暗号化装置であって、

初段では入力された64ビットの平文ブロックデータを、2段目以降では前段での処理が施された64ビットのブロックデータを入力とし、該ブロックデータを2分割した2組の32ビット・データに対してそれぞれ局所的な線形拡散処理および非線形変換処理を施し出力する2つの第1の非線形変換処理部と、これら2つの第1の非線形変換処理部からそれぞれ出力された2組の32ビット・データを連結した64ビットのブロックデータに対して最大距離分離行列を用いて線形拡散処理を施し次段へ出力する第1の拡散処理部とを、1段分の段構成として、該段構成を所定段数分接続し、

最後の前記第1の拡散処理部の後段に、この第1の拡散処理部から出力される64ビットのブロックデータを入力とする前記2つの第1の非線形変換処理部を接続し、

この2つの第1の非線形変換処理部の後段に、これら2つの第1の非線形変換処理部からそれぞれ出力された2組の32ビット・データを連結した64ビットのブロックデータに対して64ビットの鍵データを加算して64ビットの暗号化されたブロックデータとして出力する第1の鍵加算部を接続して構成されるとともに、

前記第1の非線形変換処理部の各々は、与えられた1組の前記32ビット・データをさらに4分割した4組の8ビット・データに対してそれぞれ8ビットの鍵データを加算する4つの第2の鍵加算部と、各第2の鍵加算部の出力に対してそれぞれ8ビットの入出力変換表を用いて非線形変換を行う4つの第2の非線形変換処理部と、これら4つの第2の非線形変換処理部からそれぞれ出力された4組の8ビット・データを連結した32ビット・データに対して最大距離分離行列を用いて線形拡散処理を施す第2の拡散処理部と、この第2の拡散処理部の後段にさらに接続された4組の前記第2の鍵加算部および第2の非線形変換処理部とを含むものであり、

前記第1の拡散処理部の各々は、前段の1つの第1の非線形変換処理部の4つの第2の非線形変換処理部からそれぞれ出力される8ビットのうちの相対応する1ビットを一纏めにした4ビットを行列演算における入力側の1つの要素とするとともに、後段の1つの第1の非線形変換処理部の4つの第2の非線形変換処理部へそれぞれ入力される8ビットのうちの相対応する1ビットを一纏めにした4ビットを行列演算における出力側の1つの要素として、 2^4 のガロア体の乗算に基づいた2行2列の行列演算またはこれと等価な回路によって線形拡散処理を行う8ビット拡散手段を、該前段及び後段の第2の非線形変換処理部についての該8ビットのうちの各ビットに対応して有し、

1つの前記8ビット拡散手段における前記 2^4 のガロア体の乗算に基づいた2行2列の行列演算またはこれと等価な回路では、前段の2つの第1の非線形変換処理手段の最終段における合計8の第2の非線形変換処理手段からの出力となる任意の1ビットと、後段の2つの第1の非線形変換処理手段の初段における合計8の第2の非線形変換処理手段へ入力となる任意の1ビットとのすべての組み合わせにおいて、前段側における当該1ビットの状態を、後段側における当該1ビ

ットへ、複数の演算経路を辿って波及させるための手段を含むものであることを特徴とする暗号化装置。

【請求項 1 4】

ブロック暗号方式による暗号化方法であって、

ブロックデータに対してそれを複数の分割した部分データごとに局所的な拡散を行う機能を含む第 1 の処理と、

前段の前記第 1 の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第 1 の処理手段へ入力する機能を含む第 2 の処理とを実行するステップを有し、

前記第 2 の処理は、前段の前記第 1 の処理手段に対する入力ブロックデータにおける少なくとも 1 つの特定ビットの状態を、後段の前記第 1 の処理手段に対する入力ブロックデータにおける少なくとも 1 つの特定ビットへ、複数の演算経路を辿って波及させるための機能を含むものであることを特徴とする暗号化方法。

【請求項 1 5】

ブロック暗号方式による暗号化プログラムを記録したコンピュータ読取り可能な記録媒体において、

ブロックデータに対してそれを複数の分割した部分データごとに局所的な拡散を行う機能を含む第 1 の処理機能と、

前段の前記第 1 の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第 1 の処理手段へ入力する機能を含む第 2 の処理機能であって、前段の第 1 の処理手段に対する入力ブロックデータにおける少なくとも 1 つの特定ビットの状態を、後段の第 1 の処理手段に対する入力ブロックデータにおける少なくとも 1 つの特定ビットへ、複数の演算経路を辿って波及させるための機能を含む第 2 の処理機能とを、コンピュータに実現させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【請求項 1 6】

ブロック暗号方式による復号装置であって、

ブロックデータに対してそれを複数の分割した部分データごとに局所的な拡散を行う機能を含む第 1 の処理手段と、

前段の前記第 1 の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第 1 の処理手段へ入力する機能を含む第 2 の処理手段とを備え、

前記第 2 の処理手段は、前段の前記第 1 の処理手段に対する入力ブロックデータにおける少なくとも 1 つの特定ビットの状態を、後段の前記第 1 の処理手段に対する入力ブロックデータにおける少なくとも 1 つの特定ビットへ、複数の演算経路を辿って波及させるための手段を含むものであることを特徴とする復号装置

【請求項 1 7】

ブロック暗号方式による復号方法であって、

ブロックデータに対してそれを複数の分割した部分データごとに局所的な拡散を行う機能を含む第 1 の処理と、

前段の前記第 1 の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第 1 の処理手段へ入力する機能を含む第 2 の処理とを実行するステップを有し、

前記第 2 の処理は、前段の前記第 1 の処理手段に対する入力ブロックデータにおける少なくとも 1 つの特定ビットの状態を、後段の前記第 1 の処理手段に対する入力ブロックデータにおける少なくとも 1 つの特定ビットへ、複数の演算経路を辿って波及させるための機能を含むものであることを特徴とする復号方法。

【請求項 1 8】

ブロック暗号方式による復号プログラムを記録したコンピュータ読取り可能な記録媒体において、

ブロックデータに対してそれを複数の分割した部分データごとに局所的な拡散を行う機能を含む第 1 の処理機能と、

前段の前記第 1 の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第 1 の処理手段へ入力する機能を含む第 2 の処理機能であって、前段の第 1 の処理手段に対する入力ブロックデータにおける少なくとも 1 つの特定ビットの状態を、後段の第 1 の処理手段に対する入力ブロックデータにおける少なくとも 1 つの特定ビットへ、複数の演算経路

を辿って波及させるための機能を含む第2の処理機能とを、コンピュータに実現させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ブロック暗号方式による暗号化装置及び暗号化方法並びに復号装置及び復号方法に関する。

【0002】

【従来の技術】

共通鍵ブロック暗号の代表的な基本構造にSPN型とFeistel型があり、各々について差分／線形解読法に対する強度評価と耐性を高める設計法が研究されている（文献[1]V.Rijmen, J.Daemen, B.Preneel, A.Bosselaers, E.DcWin, "The Cipher SHARK," Fast Software Encryption, LNCS 1039,1996.、文献[2]青木和麻呂,太田和夫,“最大平均差分確率および最大平均線形確率のより厳密な評価,” SCIS 96-4A,1996.、文献[3]松井充,“ブロック暗号MISTY,” ISEC 96-11,1996.）。SPN構造では、活性S-box数の保証が出来るので、設定した強度を達成するための段数決定がしやすい（文献[1]）。しかし、ブロック・サイズが大きくなりS-boxの並列度が上がると、拡散層の処理が複雑になり、速度が低下する傾向がある。

【0003】

この点を改善したのが、SQUARE/Rijndael型の暗号である（文献[4]J.Daemen, L.R.Knudsen, V.Rijmen, "The Block Cipher Square," Fast Software Encryption, LNCS 1267,1997.、文献[5]J.Daemen, V.Rijmen, "AES Proposal: Rijndael," <http://www.east.kuleuven.ac.be/~rijmen/rijndael/rijndael.docV2.zip>）。この型の暗号では、16個の並列S-boxを4×4の行列状に並べて線形拡散を同一列内に制限することで処理を軽減している。また、線形拡散にバイト位置の並べ替えを組み合わせることで、ある段の1バイトの影響は2段後に全バイトに広がり、4段で活性S-box数は25以上を達成している。

【0004】

しかしながら、同一列内のバイトが次の段で混合しないという性質があるため、SQUARE 攻撃という専用の攻撃法が存在する（文献[1]、文献[5]）。これは、拡散層が1種類という制約下で、強度と効率の両立を目指した結果と考えることが出来る。

【0005】

【発明が解決しようとする課題】

SPN型構造は、活性S-box数の下限の見積もりが容易で、差分／線形解読法に対する強度を保証した設計が可能である。しかしながら、平文／暗号文のブロック・サイズの増加に従い、S-boxの並列度が高くなると、拡散層の結合部の計算コストも高くなるという欠点があった。また、拡散層の設計によってデータ攪拌が均一でなくなる可能性があった。

【0006】

本発明は、上記事情を考慮してなされたもので、計算コストを抑えたまま高く均一な拡散を可能とする暗号化装置及び暗号化方法並びに復号装置及び復号方法を提供することを目的とする。

【0007】

【課題を解決するための手段】

本発明は、ブロック暗号方式による暗号化装置であって、ブロックデータに対してそれを複数に分割した部分データごとに局所的な拡散を行う機能を含む第1の処理手段と、前段の前記第1の処理手段から出力されるブロックデータに対してそのブロック幅にわたる線形拡散処理を行って後段の前記第1の処理手段へ入力する機能を含む第2の処理手段とを備え、前記第2の処理手段は、前段の前記第1の処理手段に対する入力ブロックデータにおける少なくとも1つの特定ビットの状態を、後段の前記第1の処理手段に対する入力ブロックデータにおける少なくとも1つの特定ビットへ、複数の演算経路を辿って波及させるための手段を含むものであることを特徴とする。

好ましくは、前記特定ビットは、各々の前記入力部分データに少なくとも1つずつ存在するようにしてもよい。

好ましくは、前記第 2 の処理手段は、前段の前記第 1 の処理手段に対する入力ブロックデータから選択した 1 ビットと、後段の前記第 1 の処理手段に対する入力ブロックデータから選択した 1 ビットとからなる全ての組み合わせ又はそのうちで所定の条件を満たす複数の組み合わせの各々について、前段側における当該 1 ビットの状態を、後段側における当該 1 ビットへ、複数の演算経路を辿って波及させるための手段を含むものであるようにしてもよい。

【 0 0 0 8 】

また、本発明は、ブロック暗号方式による暗号化装置であって、ブロックデータを複数の分割した各分割部分データに対してそれぞれ非線形変換処理を施す並列させた複数の第 1 の非線形変換処理手段の一群と、ブロックデータのブロック幅にわたる線形拡散処理を施す第 1 の線形拡散処理手段とを備え、前記第 1 の非線形変換処理手段は、前記部分データのデータ幅をさらに複数の分割した各再分割部分データに対してそれぞれ非線形変換処理を施す並列させた複数の第 2 の非線形変換処理手段の一群と、前記部分データのデータ幅にわたる線形拡散処理を施す第 2 の線形拡散処理手段とを含むものであり、前記第 1 の線形拡散処理手段は、前段の複数の第 1 の非線形変換処理手段の各々の最終段に並列させた複数の第 2 の非線形変換処理手段の各々から出力される全再分割部分データからなるブロックデータに線形拡散処理を施して後段の複数の第 1 の非線形変換処理手段の各々の初段に並列させた複数の第 2 の非線形変換処理手段の一群の各々へ各再分割部分データとして入力するものであるとともに、後段の複数の第 1 の非線形変換処理手段の初段の複数の第 2 の非線形変換処理手段への入力となる複数の再分割部分データのうちの少なくとも 1 つを、前段のいずれか同一の第 1 の非線形変換処理手段の最終段の複数の第 2 の非線形変換処理手段から出力される複数の再分割部分データのうちの少なくとも 2 つに基づいて求めることを特徴とする。

好ましくは、前記第 1 の線形拡散処理手段は、後段の全第 1 の非線形変換処理手段の各々について、当該後段の第 1 の非線形変換処理手段の初段の複数の第 2 の非線形変換処理手段への入力となる複数の再分割部分データのうちの少なくとも 1 つを、前段の各第 1 の非線形変換処理手段ごとにその最終段の複数の第 2 の非線形変換処理手段から出力される複数の再分割部分データのうちから少なくと

も2つずつ選択された再分割部分データ群に基づいて求めるようにしてもよい。

好ましくは、前記第1の線形拡散処理手段は、後段の各第1の非線形変換処理手段の初段の各第2の非線形変換処理手段への入力となる各再分割部分データを、それぞれ、前段の各第1の非線形変換処理手段ごとにその最終段の複数の第2の非線形変換処理手段から出力される複数の再分割部分データのうちから少なくとも2つずつ選択された再分割部分データ群に基づいて求めるようにしてもよい。

【0009】

なお、暗号化装置に係る本発明は、暗号方法に係る発明、復号装置に係る発明、復号方法に係る発明としても成立する（もちろん、従属項についても同様である）。

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0010】

本発明では、局所的なデータ拡散を行う小型の拡散層とブロック幅に及ぶ拡散を行う大型の拡散層を交互に重ねて運用する。本発明によれば、複数種類の異なる拡散（例えば、大小2段階の拡散）によって、計算コストを抑えたまま高く均一な拡散を実現した。また、階層的にブランチ数が保証でき（ブランチ数の階層性）、活性S-box数の下限を容易に保証できる。また、強度評価がしやすいという特性がある。

【0011】

SQUARE暗号やRijndael暗号では、小型の拡散とバイト単位の並べ方によって同等の効果を実現している。しかし、それらの暗号では拡散層が1種類であるため、SQUARE攻撃と呼ばれる解読法が存在する。本発明では、大小2種類の拡散層の組み合わせ方によって、SQUARE攻撃に対する耐性の

向上が可能である。

【0012】

また、大型の拡散層の構造を工夫することによって、例えば、その前段のS-boxと後段のS-boxとの間の組み合わせの全部または一部について、差分経路を複線化することによって、高いなだれ効果が得られ、より効果的なSQUARE攻撃に対する耐性の向上が可能になる。

【0013】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【0014】

本実施形態では、局所的な拡散（小拡散）と、ブロック幅に渡る拡散（大拡散）との組み合わせによる、入れ子型（再帰的）SPN構造の暗号方式について説明する。

【0015】

以下では、暗号化を中心に説明し、その後で復号について説明する。なお、復号アルゴリズムは、暗号アルゴリズムの逆変換であり、鍵は暗号化と復号で共通の、秘密の鍵である。

【0016】

また、本暗号方式は、ハードウェアによってもソフトウェアによっても実現可能であり、以下に示す構成例は、暗号化装置（復号装置）の機能ブロック図としても成立し、また暗号アルゴリズム（復号アルゴリズム）の機能モジュール図としても成立する。

【0017】

図1に、入れ子型（再帰的）SPN構造の暗号方式（暗号化装置（もしくは復号装置）または暗号アルゴリズム（もしくは復号アルゴリズム）、暗号処理装置）の基本的な構成例を示す。

【0018】

図1に示されるように、入れ子型SPN構造では、各段において複数並列に並んだ非線形変換モジュール（後述の例では拡大S-box）2の各々により局所

的な小拡散を行い、次いで拡散モジュール（後述の例では大MDS）3によりブロック幅に渡る大拡散を行い、また非線形変換モジュール2により局所的な小拡散を行い、ということを所定段数繰り返す。さらに、非線形変換モジュール2は、非線形変換モジュール（後述の例ではS-box）4と拡散モジュール（後述の例では小MDS）5とを交互に配列して構成される。

【0019】

すなわち、本実施形態の入れ子型SPN構造は、通常のSPN構造のS-boxの部分に小型のSPN構造（後述の例では2段のSPN構造）を再帰的に埋め込んだものである。

【0020】

このような入れ子型SPN構造によれば、ブランチ数が階層的に保証でき（ブランチ数の階層性）、活性S-box数の下限を容易に保証できる、という優れた特質が得られる。また、入れ子型SPN構造には、この他に、単純明快な構造のため、強度評価がしやすいという特性がある。

【0021】

なお、図1では、局所的な小拡散を4並列で表しているが、これに限定されるものではなく、それ以外の並列数も可能である。

また、図1では、全ブロック長を均等に分割した複数の小拡散を並列されているが、これに限定されるものではなく、異なるビット長の小拡散を複数組み合わせることも可能である。また、この場合に、全ての小拡散のビット長を異なるようにしてもよいし、一部の小拡散のビット長は同じであってもよい。

また、図1では、1種類の局所的な小拡散を用いているが、2種類以上の局所的な小拡散を用いることも可能である（例えば、図1において、ブロック幅に渡る拡散モジュール3を、1つおきに、2つの非線形変換モジュール2に渡る拡散モジュールに替えた構成）。

また、同一構成の繰り返し構造にする方法の他に、一部のみ構成を替えることも可能である。

また、例えば、全ての非線形変換モジュール2の構成を同一構成にすることも、非線形変換モジュール2について、異なる構成を混在させることも可能である

。この点は、拡散モジュール 3、非線形変換モジュール 4、拡散モジュール 5 のそれぞれについても同様である。

また、例えば、最初の入力段と、最後の出力段だけ、他の中間段とは異なる内部構成にしてもよい。

また、図 1 では、2 階層の入れ子構造であるが、3 階層以上の入れ子構造も可能である（3 階層の場合、例えば、非線形変換モジュール 4 をさらに S P N 構造にする）。また、例えば、非線形変換モジュール 2 によって階層構造を異ならせることも可能である。

この他にも、種々のバリエーションが考えられる。

【0 0 2 2】

以下では、8 ビット S - b o x を利用した A E S 相当の 1 2 8 ビット・ブロック暗号の具体例を用いつつ本実施形態について説明する。

【0 0 2 3】

ここで、ブロック暗号の強度評価に関して説明する。

【0 0 2 4】

与えられた関数 f の暗号強度を見積もる重要な指標として最大差分確率／最大線形確率がある。

【0 0 2 5】

[最大差分確率、最大線形確率の定義]

関数 $f(x)$ に対し、最大差分確率 d_p^f と最大線形確率 l_p^f はそれぞれ次式で表される。

【0 0 2 6】

【数 1】

$$d_p^f \equiv \max_{\Delta x \neq 0, \Delta y} \left| \frac{\#\{x \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^n} \right|$$

$$l_p^f \equiv \max_{\Gamma x, \Gamma y \neq 0} \left| 2 \frac{\#\{x \mid x \cdot \Gamma x = f(x) \cdot \Gamma y\}}{2^n} - 1 \right|$$

【0027】

ここで、 Δx は x の入力差分、 Γx は x のマスク値を表す。

【0028】

一般には、最大差分確率 d_p^f や最大線形確率 l_p^f を求めることが困難な場合が多い。ここで、その近似値として最大差分特性確率 DP^f および最大線形特性確率 LP^f で安全性を評価する。

【0029】

本実施形態では、入れ子型SPN構造を暗号化関数として用いる。ここでは、その基本構造であるSPS構造の特性について述べる。ここで、SPSとは、S-box層と拡散層PをS-P-Sのように3層重ねた構造を指す。

【0030】

[ブランチ数]

SPS構造において入力 x に対する拡散層の出力が $\theta(x)$ のとき、差分解読に対するブランチ数 B は次式で定義する（文献[1]、文献[6]清水秀夫,金子敏信,“共通鍵暗号のdiffusion層について,” SCIS 99-72,1999.）。

【0031】

[数2]

$$B \equiv \min_{\Delta x \neq 0} (w(\Delta x) + w(\theta(\Delta x)))$$

【0032】

ここで、 $w()$ はS-boxのビット幅を符号長としたハミング距離である。非零の入出力差分に接続するS-boxを活性S-boxと呼ぶ。

【0033】

この拡散層の入出力にS-boxを接続した構造をSPS構造と呼ぶ。S-boxが全単射のとき、SPS構造への入力ビットに非零の差分を持つものが1個でもあれば、ブランチ数の定義により、活性S-boxはブランチ数以上（すなわち B 以上）になる。また、S-boxの最大差分確率を p_s とすると、SPS構造の最大差分特性確率は、上界値 p_s^B を越えない。

【0034】

[MDS (Maximum Distance Separable) 行列]

SPS構造のS層としてM並列のS-boxを用いた場合、それらを結合する拡散層のブランチ数は $(M+1)$ 以下であり、ブランチ数が $(M+1)$ を満たす線形変換をMDS (Maximum Distance Separable; 最大距離分離) 行列と呼ぶ。

【0035】

拡散層がMDS行列であるとき、SPS構造の最大差分特性確率は上界値 p_s^{M+1} を越えない[1]。同様に、S-boxの最大線形確率を q_s とすると、SPS構造の最大線形特性確率は q_s^{M+1} を越えない。

【0036】

[入れ子型SPS構造のブランチ数]

2段SPN構造をそれより大きなSPN構造のS-boxとして利用するとき、拡大S-box (小構造) と呼ぶことにする。ここで、S-boxは M_1 並列であり、拡大S-box内の拡散層のブランチ数を B_1 とする。拡大S-boxに対する M_2 並列の2段SPN構造 (大構造) を考え、その拡散層のブランチ数を B_2 とする。このとき、大構造中の活性S-box数は下界値 $B_1 \cdot B_2$ を下回らない。この性質がブランチ数の階層性である。

【0037】

また、大小2種類の拡散層の両方がMDS行列であるとき、活性S-box数は $(M_1 + 1)(M_2 + 1)$ を下回らない。これにより、入れ子型SPN構造の DP^f 、 LP^f の上限を抑えることが可能になる。

【0038】

図2に、 $M_1 = M_2 = 4$ の場合の例を示す。15が後述する大MDS行列による拡散部を示し、11~14がその入力側の拡大S-boxを示し、16~19がその出力側の拡大S-boxを示し、各々の拡大S-box内において、20が後述する小MDSによる拡散部を示し、図中で最も小さく示した矩形(21, 22)が入力側および出力側のS-boxを示す。

【0039】

図2において、S-boxのうちハッチングしたものは活性を表し（図中の21参照）、白抜きで示したものは差分零を表す（図中の22参照）。また、太線で示した拡大S-box（11, 13, 16, 17, 19）は活性を表し、その他の拡大S-box（12, 14, 18）は差分零を表す。4段で活性S-boxが25個以上であることが分かる。

【0040】

このように、本例の暗号では、2段で $5 \times 5 = 25$ 個以上の活性S-box数を保証できる。S-boxの最大差分確率は、

$$p_s = 6 / 256,$$

2段での差分特性確率は、

$$p_s^{25} = 2^{-135.4} << 2^{-128},$$

となり、差分解読法が有効でないことが分かる。

【0041】

同様に、線形特性確率についても、

$$q_s = 22 / 256,$$

$$q_s^{25} = 2^{-88.5} << 2^{-64},$$

となり、線形解読法が有効でないことが分かる。

【0042】

なお、従来のSQUARE/Rijndael型暗号に適用されるSQUARE攻撃は、段内の1バイトに対して、他の入力を固定したまま、 2^8 通りのすべてのパターンを入力したとき、2段通過後の出力バイトの各々に対して 2^8 通りのすべてのパターンが出現する特性を利用するものであるが、本例の暗号では、例えば後述する大MDSの取り方によってS-box間の攪拌性を向上させることで、その単純な適用を困難にしている。

【0043】

以下では、入れ子型暗号方式の具体例を用いながら本実施形態についてより詳しく説明する。

【0044】

本実施形態の具体例の構成について説明する。

【0045】

図3に、本実施形態の入れ子型暗号方式のデータ攪拌部の階層構造の例を示す。

【0046】

ブロック長は、128ビットを例にとる（もちろん、他のブロック長でも本発明は実施可能である）。

鍵長は、256ビットを例にとる（もちろん、他の鍵長でも本発明は実施可能である）。なお、本実施形態で、ブロック長を128ビットとしたときに、鍵長を128ビットや192ビットとした場合について後述する。

【0047】

複数並列された拡大S-boxと大MDSとの対（ただし、後述するように最終段は大MDSを含まない）を1段と数えるものとした場合に、段数をR段として表し、具体例を用いる場合には $R=8$ を用いる。なお、基本的には段数は何段でも実施可能であるが、実際の段数は、例えば安全性や計算機資源等を想定して適宜設定することができ、好ましくは6段以上、より好ましくは8段以上とすると、より効果的である。

【0048】

なお、本例の暗号では、段関数がS-box層を2層含んでいるので、1段が通常の2段に相当する。段構造内の大MDSについては、異なるガロア体に基づくいくつかの実装を示す（強度優先や速度優先の例を挙げる）。

【0049】

図4に、本実施形態に係る暗号化装置の構成例を示す。

【0050】

101が各段であり、104は大MDS拡散層、102は拡大S-box層、103は各々の拡大S-boxである。105は、排他的論理和部である。121～124は、詳しくは後述する鍵スケジュール部の構成部分である。Pは入力となる128ビットの平文データ、Cは出力となる128ビットの暗号文データである。

【0051】

段関数は、以下に述べるように、2段SPN構造からなる32ビット処理サブ・ブロック（拡大S-box）103を4個並列に並べ、MDS拡散層104で繋いだ構造である。全体の基本構造は、この段関数の繰り返しにする。

【0052】

なお、図4の例では、暗号化と復号の処理を対称的にするため、最終段は拡大S-box層102とその後の鍵加算105だけで構成することになっている。

【0053】

段関数1段に2段SPN構造が埋め込まれ、最後に鍵加算が行われるので、拡大鍵のビット長は、 $2 \times 128 \times R + 128 = 128(2R + 1)$ となる。R=8の場合には、 128×17 ビットとなる。

【0054】

次に、S-boxについて説明する。

【0055】

本例の暗号では、入出力表で定義する8ビットS-boxを利用する。

【0056】

図5に、8ビットS-boxの入出力表の一例を示す。図5において、配列要素は16進数で表現してある。

【0057】

図5の表は、最左上の値(72)がs[0]に対応し、その1つ右の値(AA)がs[1]に対応し、その行の右端の値(9F)がs[15]に対応し、次の行に移って、その左端の値(69)がs[16]に対応し、その1つ右の値(6A)がs[17]に対応し、以下同様の要領である。そして、最下右の値(57)がs[255]に対応する。

【0058】

図5に例示したS-boxの特性は、次の通りである。

- ・ 最大差分確率：6/256（理論的最小値は4/256）
- ・ 最大線形確率：22/256（理論的最小値は16/256）
- ・ 代数次数：7次（全単射関数の最大値）

なお、 $S-box$ には、入出力表を用いる代わりに、演算処理を用いても良い。

【0059】

次に、各々の拡大 $S-box$ （または小構造とも呼ぶ）の部分について説明する。

【0060】

図6に、拡大 $S-box103$ の内部構成例を示す。この例では、4並列の8ビット $S-box112$ （図5参照）を2組用意し、拡散層113を挟んだ2段SPN構造になっている。この構造は、SPS構造と呼ぶべきものでもあるが、2段目の拡散層が省略された特殊な2段SPN構造とみなす。 $S-box112$ の入力直前では、必ず鍵加算111を行う。拡大 $S-box$ 内の拡散層113には、MDS行列を使用し、これを小MDSと呼び、 MDS_S と表記する。小MDSのブランチ数は5である。

【0061】

図7に、本例の暗号で利用する MDS_S 行列の一例を示す。図7において、行列要素は16進数で表現してある。ここで、 $S-box$ 入出力と行列要素は、乗算の際、ガロア体 $GF(2^8)$ の元とみなす。この例の場合の原始多項式は、 $x^8 + x^6 + x^5 + x + 1$ である。

【0062】

次に、本例の暗号の段関数である大構造について説明する。

【0063】

図8に、1段の部分の構成例を示す。本例の暗号の段関数である大構造は、4並列の32ビット拡大 $S-box103$ （図6参照）をMDS行列の拡散層104で結合して構成する。この段関数である大構造における拡散層104にも、MDS行列を使用し、これを大MDSと呼び、 MDS_L と表記する。ただし、ここでのMDS行列とは、拡大 $S-box$ に着目したブランチ数が5であることを意味する。

【0064】

大MDSの最も単純な構成は、拡大 $S-box$ の32ビット幅の出力を $GF($

2^{32}) の元として実現する方法である。この方法は高い強度が実現しやすいが、一般的な実行は困難もしくは高速化はしにくい。そこで、この場合には、大MDS行列に制約を課すのが好ましい。

【 0 0 6 5 】

また、4 並列のMDSを構成するには、4 ビット幅で十分であり、 $GF(2^4)$ 上の演算を利用して実現できる。さらに、MDSを巡回的なものにすることで、効率的な計算が可能になる。

【 0 0 6 6 】

また、実際には、これ以外の $GF(2^8)$ や $GF(2^{16})$ を利用する中間の型も可能である。

【 0 0 6 7 】

$GF(2^{32})$ を利用した大MDSについて説明する。

【 0 0 6 8 】

この場合、拡大S-boxの入出力を $GF(2^{32})$ の元とみなして、大構造MDSを設計する。これは、SPN構造での自然な設計法である。しかし、32 ビット幅では乗算表による実装は現実的ではない。計算による場合も一般のMDS行列では計算量が掛かり高速化が困難である。計算量が増加する原因は、ガロア体上の乗算における桁上がり時の処理が重いためである。計算量を抑えるためには、大MDS行列を、ビット表現で32ビット中の下位5ビットにのみ1が現れる(下位5ビット以外は0のものに限定した)要素で構成する方法がある。このような条件を満たす行列を使用することで、桁上がり処理を上位4ビットを入力とする表引きで処理可能となる。

【 0 0 6 9 】

図9に、大MDS行列の一例を示す。この例の場合の原始多項式は、 $x^{32} + x^{28} + x^{27} + x + 1$ である。

【 0 0 7 0 】

$GF(2^4)$ を利用した大MDSについて説明する。

【 0 0 7 1 】

図10に、この場合のMDS行列の一例を示す。この例の場合の原始多項式は

、 $x^4 + x + 1$ とする。

【0072】

ここでは、1つの拡大S-box103において4つのS-boxの各々の出力すなわち8ビット・データの同じ位置（例えば図10では最上位ビットを例にとって示している）の1ビットを集めて、これを1組4ビットのデータとし、4つの拡大S-box103からの4組の4ビット・データを、 $GF(2^4)$ の元とみなす。

【0073】

そして、8ビット・データの同じ位置について、2段の4並列拡大S-box層の間の拡散層104に4行4列のMDS行列（例えば図10では最上位ビットの場合、 $104-1$ ）を用いる。

【0074】

出力となった4組の4ビット・データは、それぞれ対応するもとの8ビット・データの同じ位置に結線される。

【0075】

S-boxのビット幅に対応して、8個のMDS行列（ $104-1 \sim 104-8$ ）を用意して、大MDSとする。

【0076】

これらの4行4列のMDS行列は、それぞれ、ブランチ数5を保証する。各MDS行列は、S-box中の異なるビット位置に接続するので、全体としてもブランチ数5を保証する。

【0077】

各拡大S-boxの同じ位置のS-box出力を単位とした表引きによって（なお、演算によってもよい）、8個のMDS行列を同時に処理する効率的な実行が可能である。

【0078】

さらに、MDS行列が巡回的な場合、32ビットごとの排他的論理和と8ビット単位のビット回転を組み合わせた効率的な処理が可能となる。

【0079】

なお、上記と同様の考え方により、8ビット・データのうちの同じ位置の2ビットごとに処理を行うこととして、各要素が8ビットの4行4列のMDS行列 ($GF(2^8)$) を、4個用意して、大MDSとすることも可能である。また、8ビット・データのうちの同じ位置の4ビットごとに処理を行うこととして、各要素が16ビットの4行4列のMDS行列 ($GF(2^{16})$) を、2個用意して、大MDSとすることも可能である。

【0080】

なお、図4では、拡大S-boxを4並列で表しているが、これに限定されるものではなく、それ以外の並列数も可能である。

また、拡大S-boxの内部構成を、全て同一とせずに、異なるものを混在させることも可能である。

また、全ての大MDS行列を同一にせずに、異なるものを混在させることも可能である。この点は、小MDS行列、S-boxの入出力表についても同様である。

また、例えば、最初の入力段と、最後の出力段だけ、他の中間段とは異なる内部構成にしてもよい。

この他にも、種々のバリエーションが考えられる。

【0081】

次に、鍵スケジュール部（鍵生成部）について説明する。

【0082】

図11に、鍵スケジュール部の構成例を示す。121は、データ攪拌部の段関数の1段分に対応する部分であり、131は線形拡散層（本例では、大MDSによる拡散層とする）であり、132は非線形変換層（本例では、4並列のSP層（S-box層・拡散層）133とする）であり、134は排他的論理和部であり、135は剰余加算部である。図11では省略しているが、121の部分の構成が必要に応じて繰り返されることになる。なお、128ビットの鍵を出力する構成単位を鍵スケジュール部の1つの段とすると、鍵スケジュール部の段数は ($2R+1$) 段となる ($R=8$ の場合、17段である)。

【0083】

図11の例では、256ビットの変形Feistel型繰り返し処理の各段の出力左半分128ビットを取り出し、段数依存定数 C_i を剰余加算して拡大鍵とする。

【0084】

なお、鍵長を256ビットとする場合には、例えば、上位128ビットを初段の線形拡散層131に与え、下位128ビットを非線形変換層132に与えればよい。また、鍵長を128ビットとする場合には、例えば、その128ビットを初段の線形拡散層131に与えるとともに、非線形変換層132に与えればよい。また、鍵長を192ビットとする場合には、例えば、上位128ビットを初段の線形拡散層131に与え、下位側64ビットと上位側64ビットとを結合した128ビットを非線形変換層132に与えればよい。

【0085】

なお、図12のように、段数依存定数 C_i を剰余加算する箇所について、種々のバリエーションが考えられる。

【0086】

図13に、図11や図12における非線形変換層132の各々の非線形変換層133の構成例を示す。141はS-boxであり、142は4並列のS-boxを入力とする小MDSである。

【0087】

なお、このS-boxは、図4の暗号処理側のS-boxと同じものでもよいし、異なるものでもよい。小MDSについても同様である。また、鍵スケジュール部の各段によってS-boxや小MDSの構成を変えることも可能である。

【0088】

図14に、図11や図12における非線形変換層132の各々の非線形変換層133の他の構成例を示す。この例は、図13の構成に対して、排他的論理和部143を付加したものである。

【0089】

さらに、図14において、S-boxに対する入力と排他的論理和をとる定数を、段数依存定数とする構成も可能である。

【0090】

次に、各段で異なる定数 C_i を作る方法の一例について説明する。

【0091】

図11や図12の鍵スケジュール部の128ビットの加算定数 C_i は、4つのビット定数(H_0, H_1, H_2, H_3)の組み合わせで記述することができる。

32ビットの定数 H_i の一例を次に示す。

$$H_0 = (5a827999)_{\text{H}} = 2^{1/2} / 4$$

$$H_1 = (6ed9ebal)_{\text{H}} = 3^{1/2} / 4$$

$$H_2 = (8f1bbcd c)_{\text{H}} = 5^{1/2} / 4$$

$$H_3 = (ca62c1d6)_{\text{H}} = 10^{1/2} / 4$$

加算定数 C_i の組み合わせを、 $C_i = (C_{i0}, C_{i1}, C_{i2}, C_{i3})$ と記述する。各段で異なる128ビットの定数 C_i を容易に生成するため、 C_i を構成する H_i の組み合わせの決定に8ビットLFSRを用いる。例えば、LFSRの原始多項式には $(1D)_{\text{H}}$ を、LFSRの初期状態には $(8B)_{\text{H}}$ を用いる。このLFSRを用いて生成されたビット列を2ビットずつ読み出し、定数として使用する32ビット定数 H_i を決定する。

【0092】

図15に、上記のような方法によりLFSRを用いて決定した加算定数表の例を示す。

【0093】

なお、LFSRの初期状態は、可変としてもよいし、固定としてもよい。前者の場合には、LFSRの初期状態も鍵の一部を構成することになる。後者の場合には、暗号側と同じLFSRの初期状態を持つ復号側のみ、暗号文を復号することができる。

【0094】

以上説明したような鍵スケジュール部によれば、非線形変換層については、入力の1ビットが変化すると、S-box(141)により、8ビットに変化を波及させ、さらに、小MDS(142)により、32ビットに変化を波及させることができる。さらにまた、線形拡散層については、大MDS(131)が前段の

非線形変換層の出力をより大きく攪拌するので、1ビットの違いも、128ビットの幅に広がる利点がある。

【0095】

従って、このような鍵スケジュール部によれば、各段でバラバラな鍵が出やすい、攪拌しやすい、という効果を得ることができる。また、段ごとに異なる定数により、段にわたる鍵の一致が少ない（鍵がほぼ一致しない）、という効果を得ることができる。

【0096】

さて、以下では、大きなブロック長を持つブロック暗号のデータの攪拌部に用いられる効率的な線形拡散装置について説明する。

【0097】

図16に、本実施形態の線形拡散装置の基本的な構成要素である有限体乗算装置の構成例を示す。前述した $GF(2^{32})$ あるいは $GF(2^{16})$ を利用した大MDS（図9、図4の104、図11や図12の131参照）における、1つの入力と大MDS行列の1つの要素との積の計算に、この線形拡散装置を用いることができる。

【0098】

図16に示されるように、この有限体乗算装置は、係数格納部202、乗算部203、桁溢れ帰還部201、排他的論理和部（排他和部）204を用いて構成される。

【0099】

係数格納部202は、係数すなわち乗算の乗数（例えば、図9の大MDS行列の1つの要素）を格納する部分である。

【0100】

乗算部203は、入力ワードと係数を2進数とみなした場合の乗算を行う部分である。

【0101】

桁溢れ帰還部201は、乗算の結果として生ずる桁溢れを有限体上の乗算に戻すため排他的論理和部204で足される数（帰還ワード）を検索する部分である

【0102】

排他的論理和部204は、乗算部203の出力と桁溢れ帰還部201の出力ビット的な排他和を行う部分である。

【0103】

有限体乗算装置200の機能は、有限体GF(2)の拡大体GF(2^k)の元である入力ワードaと同じ有限体の別の元である係数bの積 $a \times b$ を出力ワードとして計算することである。

【0104】

まず、有限体における積について説明する。

【0105】

なお、以下の記述において、 $\sum a_i x^i$ において総和を取るiの範囲や $\sum b_j x^j$ において総和を取るjの範囲を $0 \sim k-1$ とし、それらの範囲についての記述を省略する。

【0106】

GF(2^k)の元は、多項式表現によって、ある変数xの $(k-1)$ 次の多項式 $\sum a_i x^i$ として表現できる。元aを表現するのに、その係数を並べて $c_{k-1} c_{k-2} \dots c_0$ として表現することもある。

【0107】

2つの元 $a = \sum a_i x^i$ と $b = \sum b_i x^i$ の積は、

$$a \times b = (\sum a_i x^i) \times (\sum b_i x^i) \mod p(x)$$

で定義される。

【0108】

ここで、 $p(x)$ はGF(2^k)の原始多項式と呼ばれ、周期 $(2^k - 1)$ を持つk次の既約なモニック多項式である。また、modの意味は、例えば、 $k=32$ の場合、原始多項式として $p(x) = x^{32} + x^{28} + x^{27} + x + 1$ を選んだ場合、多項式の積によって x^{32} の項や因子が現れた場合には、それを $(x^{28} + x^{27} + x + 1)$ と見なすということを表す。従って、積もまたk次未満の多項式となる。

【 0 1 0 9 】

一般に、このような操作を行う場合、高速な処理を行うため、乗数と被乗数をタグとして積を検索する乗算表を用いた乗算装置を用いることがある。しかし、乗数と被乗数はともに 2^k 個の値を取り得るので、乗算表は、 2^{2k} 個のエントリを持ち、各エントリは k ビットのサイズを持つので、 k がある程度大きくなると、乗算表のサイズは非常に大きなものとなる。

【 0 1 1 0 】

本実施形態も、基本的には、乗算表を用いる方式に類似するが、係数がある制約条件を満足する場合には、はるかに小さな記憶容量によって実現することができる。

【 0 1 1 1 】

その制約条件とは、係数 b は、定数であって、非零の係数を持つのは、ある次数 t 以下の下位の係数のみであるということである（ t 次を越える次数の係数は 0 であり、 t 次以下の係数は 0 または 1 である）。ある元 a が任意の元を取る場合には、桁溢れは、最大 32 ビットであるが、この制約条件を満足する場合には、桁溢れは、高々、 t ビットである。この t ビットの桁溢れの値を決定するのは、被乗数 a の上位 t ビットまでの MSB (Most Significant Bits) である。

【 0 1 1 2 】

有限体上の乗算と通常が多項式と見なした場合の乗算との違いは、2 進数の積の結果、32 次以上の係数への桁溢れが起こった場合に、原始多項式によって、32 次未満の係数へその寄与を還元する必要があるが、本実施形態では、桁溢れ帰還部 201 が、還元すべきワードを表として持っている。

【 0 1 1 3 】

この帰還ワードは、高々 $(t+1)$ ビットの係数 b と乗数 a の上位 t ビットと原始多項式から決定できる。つまり、 $(a[(k-t) \dots (k-1)] \times b)[(t+1) \dots 2t] \bmod p(x)$ によって与えられる。ここで、 $a[(k-t) \dots (k-1)]$ とは、 a の中から、 $(k-1)$ 次から $(k-t)$ 次までの項を取り出したものである。

【0 1 1 4】

すなわち、桁溢れ帰還部 2 0 1 が持つ帰還ワードの表の内容は、対応する MDS 行列（図 9 参照）の要素に応じて決まる。

【0 1 1 5】

桁溢れ帰還部 2 0 1 が持つ帰還ワードの表は、 2^t 個のエントリからなり、各エントリは k ビットのサイズを持つ。

【0 1 1 6】

次に、上述した有限体乗算装置を利用することで実現される、ブロック暗号のデータ・ブロックに線形変換を施す線形変換装置について説明する。

【0 1 1 7】

線形変換の 1 種に MDS 行列による線形変換がある。MDS 行列とは、データ・ブロックが、複数 (n) のワードから構成され、各ワードが k ビットの長さを持つ場合、各ワードを有限体 $GF(2^k)$ の元と見なし、 n 個の元の組を n 個の元の組に線形写像する n 行 n 列の行列であって、すべての小行列が非零のものである。MDS 行列による線形変換は、非零の入出力のワードの数の下限が保証されているという性質を持つ。

【0 1 1 8】

しかし、一般に、有限体 $GF(2^k)$ 上の行列演算は、 $GF(2^k)$ 上の複数回の乗算と加算から構成され、計算コストが大きい。

【0 1 1 9】

図 1 7 に、本実施形態の線形変換装置の構成例を示す。前述した $GF(2^{32})$ あるいは $GF(2^{16})$ を利用した大 MDS（図 9、図 4 の 1 0 4、図 1 1 や図 1 2 の 1 3 1）に、この線形変換装置を用いることができる。

【0 1 2 0】

図 1 7 の構成では、まず、図 1 6 の有限体乗算装置を MDS 行列に対応してマトリクス状に用意する。

【0 1 2 1】

図 1 7 において $m = n$ とすると、 n^2 個の有限体乗算装置 2 0 0 の各々の係数は、 n 行 n 列の MDS 行列の対応する要素と同じ値をとる。係数 a_{ij} を持つ装置

には、第 i 入力ワードが入力される。

【0 1 2 2】

各々の出力ワードに対する排他的論理和部（排他和部）205は、それぞれ、ある j に対応する係数 a_{ij} を持つすべての有限体乗算装置200の出力ビット的な排他的論理和を計算し、第 j 出力ワードとして出力する。

【0 1 2 3】

本実施形態における線形変換装置は、線形変換を表現するMDS行列を (a_{ij}) で表現するとき、各要素 a_{ij} は高々 t 次までの項しか非零の係数を持たないことを特徴とする。ここで、 i, j は、0から $n-1$ までの整数値を取りうるとする。また、 t は、有限体 $GF(2^k)$ の拡大次数 k よりも小さな正数であるとする。

【0 1 2 4】

これによって、図18のような乗算が実現できる。

【0 1 2 5】

なお、桁溢れ帰還部201が持つ帰還ワードの表の内容は、対応するMDS行列の要素に応じて決まるので、例えば、図9の大MDS行列の例では、4種類の帰還ワード表だけ持てばよいことになる。

【0 1 2 6】

次に、本暗号方式に用いるMDS行列（特に大MDS）を生成するためのMDS行列生成装置（もしくはランダム生成アルゴリズム）について説明する。

【0 1 2 7】

図19に、MDS行列生成装置の構成例を示す。図19に示されるように、このMDS行列生成装置は、要素生成部231、小行列式計算部232、判定部233を用いて構成される。

【0 1 2 8】

図20に、この場合の手順の一例を示す。

【0 1 2 9】

要素生成部231は、ランダムに、 n 行 n 列のMDS行列の各行列要素を生成する（ステップS1）。なお、先の有限体乗算装置を適用可能とする場合には、

このときに、下位 t ビットのみ非零の要素（ t 次以下の要素）からなるMDS行列を生成しておく（すなわち、この場合には、要素生成部231内で、下位 t ビットのみ非零かどうかのチェックを行うことになる）。

【0130】

なお、行列要素を生成するためには、乱数を発生して用いる方法や、多重ループの制御変数の値を用いる方法など種々の方法が考えられる。

【0131】

次に、小行列式計算部232は、要素生成部231の生成した行列の1次小行列を計算し（ステップS2）、判定部233は、小行列式計算部232が計算した小行列が非零か否かを判定する（ステップS3）。1つでも零の1次小行列式があれば、ステップS1からやり直す。

【0132】

すべての1次小行列式が非零ならば、同じ要領で、2次小行列について同様にチェックする（ステップS4、S5）。

【0133】

以上を、 n 次小行列式まで、同じ要領で行い（ステップS6、S7）、1次から n 次まですべての小行列式が非零であることが確認されたならば、そのMDS行列を出力する（ステップS8）。

【0134】

なお、ステップS8で得たMDS行列を暗号化に用いるMDS行列とした場合、復号に用いるMDS行列は、ステップS8で得たMDS行列の逆行列によって与えられる（逆に、ステップS8で得たMDS行列を復号に用いる場合には、その逆行列が、暗号化に用いるMDS行列となる）。

【0135】

ただし、ステップS8で得られたMDS行列の全ての要素が下位 t ビットのみ非零であっても、その逆行列の全ての要素が下位 t ビットのみ非零であるとは限らない。

【0136】

なお、図20の手順において、小行列式の判定を1次から n 次まで順番に行って

いるが、他の順番でもよく、また、それらの全部または一部を並列して行ってもよい。

【0137】

次に、暗号化に用いるMDS行列と、その逆行列である、復号に用いるMDS行列との両方とも、下位 t ビットのみ非零という条件を満たすように、MDS行列を求める方法について説明する。

【0138】

図21に、この場合のMDS行列生成装置の構成例を示す。図21に示されるように、このMDS行列生成装置は、要素生成部231、小行列式計算部232、判定部233、逆行列生成部234、逆行列判定部235を用いて構成される。要素生成部231、小行列式計算部232、判定部233の部分は、図19と同様である。

【0139】

図22に、この場合の手順の一例を示す。

【0140】

まず、先の例と同様にして、要素生成部231、小行列式計算部232、判定部233により、下位 t ビットのみ非零の要素からなるMDS行列を生成する（ステップS11）。

【0141】

次に、逆行列生成部234により、生成されたMDS行列の逆行列を求める（ステップS12）。

【0142】

次に、逆行列判定部235は、求められた逆行列の各々の要素が、下位 t ビットのみ非零かどうか調べる。

【0143】

全ての要素が下位 t ビットのみ非零であれば（ステップS13）、そのMDS行列および逆行列を出力する（ステップS14）。

【0144】

1つでも下位 t ビットのみ非零ではない要素があれば（ステップS13）、S

1 1 からやり直す。

【 0 1 4 5 】

なお、ステップ S 1 1 で生成された M D S 行列を暗号化に用いる場合、ステップ S 1 2 で生成された逆行列を復号に用いることになる（逆に、ステップ S 1 1 で生成された M D S 行列を復号に用いる場合、ステップ S 1 2 で生成された逆行列を暗号化に用いることになる）。

【 0 1 4 6 】

なお、M D S 行列を生成するにあたっては、同一行内に同じ値の要素が存在しないような M D S 行列（ n 行 n 列の M D S 行列において第 $i 1$ 要素から第 $i n$ 要素までの中に同一の値を持つ 2 個以上の要素がないもの）を生成するようにしてもよい。例えば、図 2 0 や図 2 2 の手順例の場合、M D S 行列の生成時に、同一行内に同じ値の要素が存在するかどうかチェックし、同一行内に 1 つでも同じ値の要素が存在すれば、M D S 行列を生成し直すようにすればよい。なお、同一列内に同じ値の要素が存在しても構わない。

【 0 1 4 7 】

ブロック暗号のデータの線形変換装置として、同一行内に同じ値の要素が存在しないような M D S 行列を選択した線形変換装置を用いることによって、入力ワードの差分値が相殺する確率を小さくすることができる。

【 0 1 4 8 】

また、同一行内の要素の和が 1 または 0 にならないように M D S 行列を生成するようにしてもよい。この場合も、同様の効果が得られる。

【 0 1 4 9 】

次に、S - b o x と小 M D S の組み合わせを選択する（あるいは最適化する）ことによって、より安全性を高める方法、より具体的には、最大差分特性確率が理論的最悪例よりも良くなることを保証する S - b o x と M D S の組み合わせの設計方法について説明する。

【 0 1 5 0 】

M D S はブランチ数 B しか保証しないので、S - b o x の最大差分確率が p とすると、最大差分特性確率は、 p^B になる。例えば、 m 行 m 列の M D S は $B = m$

+1となる。しかし、S-boxと小MDSの組み合わせを選択する（あるいは最適化する）ことにより、ブランチ数Bで、最大差分特性確率が p^B 未満を保証することができる。この結果、通常のMDSよりも最大差分確率が小さいMDSとS-boxを組み合わせることにより、相乗効果が望め、安全性をより向上させることができる。

【0151】

さて、暗号アルゴリズムの安全性評価の一手法として、差分解読法あるいは線形解読法があり、両者は双対な関係にある。差分解読法に着目すると、S-boxの安全性は入出力の差分相関を持つ確率で規定され、この確率が小さいほど安全性が高い。暗号アルゴリズムでは、差分確率の小さいS-boxが多数組み合わせられるほど安全性が向上する。効率的なS-boxの連結方法として、線形変換装置が従来から提案されている。線形変換装置は、あるブロック長のデータに対して線形変換を施す装置で、暗号化装置（や復号装置）の構成要素として利用されることがある。線形変換の一種にMDS行列による線形変換がある。

【0152】

MDS行列とは、データブロックがn個の複数のワードから構成される場合、n個のワードへの線形変換を定義する行列であり、非零の入出力ワードはn+1個以上が保証されているという性質を持つ。しかし、S-boxは、差分確率として、 $6/256$ 、 $4/256$ 、 $2/256$ など複数の値の候補を持つため、MDSであっても、n+1個の確率がそれぞれ $6/256$ のMDSと、それぞれ $4/256$ であるMDSとでは、後者の方が安全性が高い。

【0153】

従来、S-boxとMDSは単体の構成要素としてそれぞれ独立に安全性を評価されたが、ここでは、S-boxとMDSの相乗効果を検証する装置の例を示す。

【0154】

図23に、この場合の処理手順の一例を示す。この例は、差分解読法に着目して、S-boxとの相乗効果が望めるMDS決定処理を示している。差分解読法と線形解読法は双対な関係にあるため、この処理を線形確率に着目して行うこと

により、線形解読法に対しても同じ効果が得られる。

【0155】

まず、複数の $S-b o x$ の候補と複数の小 $M D S$ の候補を生成する（ステップ $S 2 1$ 、ステップ $S 2 2$ ）。なお、ステップ $S 2 1$ とステップ $S 2 2$ は逆の順番で行ってもよいし、並列して行ってもよい。

【0156】

次に、 $S-b o x$ 候補のなかから $S-b o x$ を 1 つ選択するとともに（ステップ $S 2 3$ ）、小 $M D S$ 候補のなかから小 $M D S$ を 1 つ選択する（ステップ $S 2 4$ ）。なお、ステップ $S 2 3$ とステップ $S 2 4$ を逆の順番で行ってもよいし、並列して行ってもよい。

【0157】

次に、後述するように、有効な（活性にした） $S-b o x$ の差分値の最大を計算し（ステップ $S 2 5$ ）、上限（例えば、 $6 / 256$ ）を下回る差分値（例えば、 $4 / 256$ ）が含まれているかどうか調べる。

【0158】

そして、含まれていれば（ステップ $S 2 6$ ）、そのときの $S-b o x$ と小 $M D S$ の組み合わせを出力する（ステップ $S 2 7$ ）。

【0159】

一方、含まれていなければ（ステップ $S 2 6$ ）、 $S-b o x$ と小 $M D S$ の一方または両方を選択し直して、以下、同様に、処理を繰り返す。

【0160】

なお、図 23 では、最初に複数の $S-b o x$ の候補と複数の小 $M D S$ の候補を生成しておいたが、その代わりに、最初の 1 組以外は、ステップ $S 2 6$ で条件を満たさずに、他の $S-b o x$ およびまたは $M D S$ を選択することになったときに、生成するようにしてもよい。

【0161】

ステップ $S 2 5$ およびステップ $S 2 6$ の処理は、実際には、次のようになる。

【0162】

例えば、図 6 の例の場合、 $S-b o x$ と小 $M D S$ の組について、次の 4 種類、

計 2 0 通りの検証を行い、すべての条件を満たした場合に、ステップ S 2 7 でそのときの S - b o x と小 M D S の組が出力される。

①小 M D S 1 1 3 の入力側の 1 つの S - b o x 1 1 2 のみ活性にした場合に、小 M D S 1 1 3 の出力側の 4 つの S - b o x 1 1 2 が全て活性になり、かつ、そのうちの 1 つでも上限を下回る差分値になれば、この検証を合格とする。この検証を、入力側の 4 つの S - b o x 1 1 2 の各々について行う（4 通りある）。

②小 M D S 1 1 3 の入力側の 2 つの S - b o x 1 1 2 のみ活性にした場合に、小 M D S 1 1 3 の出力側の 4 つの S - b o x 1 1 2 が全て活性になれば、この検証を合格とし、小 M D S 1 1 3 の出力側の 3 つの S - b o x 1 1 2 が活性になり、かつ、そのうちの 1 つでも上限を下回る差分値になれば、この検証を合格とする。この検証を、入力側の 2 つの S - b o x 1 1 2 の組み合わせの各々について行う（6 通りある）。

③小 M D S 1 1 3 の出力側の 2 つの S - b o x 1 1 2 のみ活性にした場合に、小 M D S 1 1 3 の入力側の 4 つの S - b o x 1 1 2 が全て活性になれば、この検証を合格とし、小 M D S 1 1 3 の入力側の 3 つの S - b o x 1 1 2 が活性になり、かつ、そのうちの 1 つでも上限を下回る差分値になれば、この検証を合格とする。この検証を、出力側の 2 つの S - b o x 1 1 2 の組み合わせの各々について行う（6 通りある）。

④小 M D S 1 1 3 の出力側の 1 つの S - b o x 1 1 2 のみ活性にした場合に、小 M D S 1 1 3 の入力側の 4 つの S - b o x 1 1 2 が全て活性になり、かつ、そのうちの 1 つでも上限を下回る差分値になれば、この検証を合格とする。この検証を、出力側の 4 つの S - b o x 1 1 2 の各々について行う（4 通りある）。

【 0 1 6 3 】

上記の複数の検証処理は、逐次行ってもよいし、全部または一部を並列的に行ってもよい。上記の複数の検証処理のうち、1 つでも合格しないものがあれば、その S - b o x と小 M D S の組み合わせについては、以降の全ての検証処理のうち切って、不合格として構わない。

【 0 1 6 4 】

なお、図 2 3 の手順の例では、最初に条件を満たした S - b o x と小 M D S の

組み合わせが得られた時点で、処理をうち切るものであったが、条件を満たした $S - box$ と小MDSの組み合わせを複数求め、それらのうちで最も良いと評価されるものを選択するようにしてもよい。

【0165】

以下では、復号側について説明する。

【0166】

復号側は、基本的には、暗号側を逆にした構造である（鍵は同一である）。

【0167】

図24に、図4の暗号化装置に対応する復号装置の構成例を示す。

【0168】

図25に、図6の小構造に対応する構成例を示す。

【0169】

図26に、図8の大構造に対応する構成例を示す。

【0170】

なお、図24では、復号装置の鍵スケジュール部は、図4の暗号化装置の鍵スケジュール部と同一の構成としてある。

【0171】

復号装置における、 $S - box1112$ の入出力表、小MDS1113の小MDS行列、大MDS1104の大MDS行列は、それぞれ、暗号化装置における、 $S - box112$ の入出力表（例えば図5）、小MDS113の小MDS行列（例えば図7）、大MDS104の大MDS行列（例えば、図9、図10）と逆関数（逆行列）の関係になっている。

【0172】

なお、図24では、鍵については、図4と同様の順番で生成しているが、図4とは逆の順番で生成するように構成することも可能である。

【0173】

図27に、この場合の鍵スケジュール部の構成例を示す。

【0174】

1132は、図11の非線形変換層132の逆変換を示している（例えば各々

のSP層133の逆変換（例えば図13あるいは図14の入出力を逆方向にしたもの）を4並列にしたものである）。

【0175】

図27の鍵スケジュール部で用いる、S-boxの入出力表、小MDS行列、大MDS行列は、それぞれ、図11の鍵スケジュール部で用いる、S-boxの入出力表、小MDS行列、大MDS行列と逆関数（逆行列）の関係になっている。

【0176】

また、図27の復号の鍵入力 K' は、図4において（暗号側で）最後の鍵加算に用いられた鍵とする。

【0177】

なお、この場合においても、段数依存定数 C_i を剰余加算する箇所について、図12の場合と同様の方法をはじめとして、種々のバリエーションが考えられる。

【0178】

以下では、大MDSの好ましい一形態について説明する。

【0179】

入れ子型（再帰的）SPN型暗号のSQUARE攻撃に対する安全性がSQUARE暗号/Rijndael暗号より改善する一つの理由として、S-box間（前段の拡大S-boxの後半（あるいは最終段）のS-boxと後段の拡大S-boxの前半（あるいは初段）のS-boxとの間）に設けた大MDS拡散層による攪拌性があげられるが、ここでは、SQUARE攻撃に対する耐性をより効果的なものにするための大MDSの構成についての選択基準の例を示す。

【0180】

ところで、通常、SPN型暗号に対するSQUARE攻撃では、

①可変byteは全256パターンを取る、

②他のbyteは固定、

という条件を満たす256パターン（ Λ 集合）を入力し、そして、256パターンに対するビット和が0になる鍵を探索することによって、鍵を推定する、とい

う手順が取られる。

【0181】

これを背景として、大MDSの結合（大MDSの入力側と出力側のビット間の結合関係あるいは演算経路の配線関係）に一定の条件を加えることによって、SQUARE攻撃に対する安全性を向上させる。この一定の条件とは、概略的には、差分経路（前段の拡大S-boxの前半のS-boxと後段の拡大S-boxの前半のS-boxとの間の演算経路）の全部または一部を複線化させる（ファン・イン（fan-in）を2以上にする）というものである。これによって、高いなだれ効果が得られ、従来に比較してSQUARE攻撃可能な段数を1段減らせることにができる。

【0182】

まず、図28～図35（各図においてデータは上側から下側へ流れるものとしている）を参照しながら、大MDSの一構成例を示す。この例は、全ての差分経路についてファン・インを2以上にするように、大MDSを構成した例である。

【0183】

なお、ここで説明する大MDSも、ハードウェア（例えば半導体基板上等に形成した実回路）によっても、機能的に等価な行列演算または入出力変換表による変換を実行するためのソフトウェアによっても実現可能であるが、図28～図35ではハードウェアによって実現する場合を想定して説明する。

【0184】

図28に、図4の暗号システムや図24の復号システムにおける大MDS層（暗号側の場合は104-1～104-8で、復号側の場合は1104-1～1104-8）と、その前段および後段の4並列の拡大S-box（暗号側の場合は103で、復号側の場合は1103）、そして拡大S-boxを構成する4並列のS-boxおよび小MDSを示す。ただし、図6等にしたような鍵加算は図28以降の各図ではその記述を省略している。

【0185】

さて、図28の例は、図10と同様に、各S-boxの8ビットのうちの1ビットを抜き出したものについてそれぞれ独立に同一処理を行う構成を取っている

。図28は、各S-boxの8ビットのうちの最も左側の1ビットを抜き出したもの（16ビットデータあるいは4組の4ビットデータ）について処理を行うMDS部分104-1について説明している。なお、図29では、各S-boxの8ビットのうちの最も右側の1ビットを抜き出したものについて処理を行うMDS部分104-8について説明している。また、図示はしていないが他の6ビットの各々についても同様である。

【0186】

図28以降の各図で示す配線やレイアウトは論理的な関係を示すものであり、実配線や実レイアウトにはもちろん設計の自由度がある。また、図28の例では、大MDS層の各部分104-1～104-8の8つを実装するものとしているが、MDS部分104-1～104-8のうちの一部（例えば、1つ、2つ、あるいは4つ）のみを実装し、それを時分割的に共用するように構成することも可能である。

【0187】

なお、暗号側と復号側で構成の仕方は同様であるので（逆変換の関係になるだけである）、以下では、暗号側を例にとって説明する。また、大MDS層の各部分104-1～104-8は同一構成として、そのうちの1つの部分（104-1とする）について説明する。

【0188】

図30に、大MDS層の一つの部分（以下、単に大MDSと呼ぶ）104-1の前段の第1の拡大S-box103-1-1の後半の4つのS-boxと、大MDSの後段の4つの拡大S-box103-2-1～103-2-4の前半における合計16のS-boxとの間の結合関係の一例を示す。なお、図30～図34において、ビットの配線が合流するところでは、排他的論理和によってそれら複数ビットが結合される（各図では、排他的論理和回路の記述を省略している）。

図31に、大MDSの前段の第2の拡大S-box103-1-2について、図30と同様の関係を示す。

図32に、大MDSの前段の第3の拡大S-box103-1-3について、

図30と同様の関係を示す。

図33に、大MDSの前段の第4の拡大S-box 103-1-4について、図30と同様の関係を示す。

図30～図33を参照すると、大MDSの後段の拡大S-boxの同一のS-boxには、いずれについても、それぞれ図30～図33のようにして排他的論理和により結合された4つのビットが結合されるが、それら4つのビットについても排他的論理和によって接合される。この様子を、大MDSの後段の第1の拡大S-box 103-2-1について、図34に示す。大MDSの後段の他の拡大S-box 103-2-2～103-2-4については図示を省略するが、同様の結合関係である。なお、ここでは図30～図33のような排他的論理和による結合の後に図34のような排他的論理和による結合を行ったように示しているが、それらすべての排他的論理和による結合を一括して行ってもよいし、適宜複数に分けて行ってもよい。

【0189】

さて、以上に例示した構成は、次の基準に基づいている。

【0190】

図4のような暗号回路において連続する2段（すなわち図30～図34）を考える。前段の拡大S-box 103における前半のS-boxと、後段の拡大S-box 103の前半のS-boxとは、前段の拡大S-box 103における後半のS-boxを経由して接続されている。このときに、次の基準を大MDS（130-1～103-8）の選択基準とする。

（1）前段の拡大S-box 103の前半における全S-box（ここでは合計16個のS-box）のうちから任意に選んだ1つのS-boxと、後段の拡大S-box 103の前半における全S-box（ここでは合計16個のS-box）のうちから任意に選んだ1つのS-boxとが、いずれもの組み合わせについても、2本以上の経路によって相互に接続（結合）されている。

（2）当該大MDSによってなされる線形拡散の逆変換もしくは逆関数（すなわち復号回路側の大MDS）が存在し、かつ、それについても（1）と同じ条件が満たされる。

(1) については、例えば、図35に示すように、1001のS-boxと1002のS-boxとが、矢印で示すような2本の経路によって相互に接続されており、他のS-box間についても同様に2～4本の経路によって相互に接続されている。なお、これに対して、従来のSQUARE暗号/Rijndael暗号では、図36に示すように、1003のS-boxと1004のS-boxとの間は矢印で示すように1本のみの経路であり（ファン・イン=1）、他のS-box間についても同様である（したがって、なだれ効果は低い）。

(2) については、後述するように満たされている。

【0191】

ここで、上記基準を満たす構成におけるSQUARE攻撃に対する安全性について説明する。

【0192】

まず、SQUARE攻撃で入力として用いる Λ （ラムダ）集合の定義を示す。

各データが n 個のバイト（ n は複数とする；なお1バイト=8ビットである）を連結したものからなり、そのようなデータを256個含む集合があり、その256個の全データにおける各々のバイトの値について、次のいずれか一方が成立するとき、

(a) 取り得る256（ $=2^8$ ）種類の値が全部現れる

(b) 取り得る256（ $=2^8$ ）種類の値のうちの1つのみが現れる（すなわち、常に値が固定）

この256個の n バイトのデータの集合を Λ 集合と呼ぶ。

Λ 集合には、次の性質がある。

・ Λ 集合を入力とする並列S-box（可逆）の出力の集合もまた、 Λ 集合である。

【0193】

値が固定でないバイトが1個だけある Λ 集合を、図30～図33のような上記基準を満たす構成における前段の拡大S-box103の後半のS-box群に入力としたとき、次の性質が確率1で成立する（図35参照）。

(i) Λ 集合となるのは、前段の拡大S-boxの後半のS-boxの出力までである。

(ii) 任意ビットの256パターンについての和が0になるのは、後段の拡大S-boxの前半のS-boxの入力位置までである。

【0194】

これに対して、従来のSQUARE暗号/Rijndael暗号では、次の性質が確率1で成立する(図36参照)。

(i') 後段の前半のS-box通過後も Λ 集合である。

(ii') 後段の後半のS-boxの入力位置の任意のビットを256パターンについて足すと0になる。

【0195】

このように、上記基準を満たす大MDSでは、従来のSQUARE暗号/Rijndael暗号に比較してS-boxの層についてみると1層分早く解読に有効な性質が壊される。つまり、ある段数のSQUARE暗号/Rijndael暗号に比べて、それより1層分少ない構成でもSQUARE攻撃に対する強度は同等と考えられる。よって、SQUARE攻撃に対する安全性は、S-box層で1層分は向上していることが分かる。

【0196】

次に、図30～図34で説明した結合関係については、種々のバリエーションが可能である。以下、この結合関係のバリエーションについて説明する。

【0197】

図30～図34において例示した大MDSの構成において、図37(a)に示すように、前段の拡大S-box103-1-1の後半の4つのS-boxから取り出した1ビットをそれぞれ $X_{11} \sim X_{14}$ で表し、これらをまとめたものを4ビットデータ X で表し、同様に、拡大S-box103-1-2、拡大S-box103-1-3、拡大S-box103-1-4、後段の拡大S-box103-2-1、拡大S-box103-2-2、拡大S-box103-2-3、拡大S-box103-2-4についても、それぞれ、 $X_{21} \sim X_{24}$ および X_2 、 $X_{31} \sim X_{34}$ および X_3 、 $X_{41} \sim X_{44}$ および X_4 、 $Y_{11} \sim Y_{14}$ および Y_1 、 $Y_{21} \sim$

Y_{24} および Y_2 、 $Y_{31} \sim Y_{34}$ および Y_3 、 $Y_{41} \sim Y_{44}$ および Y_4 で表すものとする。

【0198】

この場合に、各拡大S-box 103に対応する4ビットデータ $X_1 \sim X_4$ 、 $Y_1 \sim Y_4$ の各々を $GF(2^4)$ の元とみなした場合に、入力側の $X_1 \sim X_4$ から出力側の $Y_1 \sim Y_4$ を求めるための大MDS行列は、図37(b)に示すようになる。

【0199】

そして、図30～図34において、前段の1つの拡大S-boxの後半の4並列のS-boxから1ビットずつ取り出した4ビットと、後段の1つの拡大S-boxの前半の4並列のS-boxから1ビットずつ取り出した4ビットとの間の結線（結線パターン）は、図37(b)に示す対応する行列要素についての $GF(2^4)$ 上の乗算の結線表現（結線パターン）になっている（図30～図34において、x5、xA、xEで示している）。すなわち、図30～図34の線形拡散と、図37(b)の線形拡散は、等価な関係にある。

【0200】

ここで、図38に、 $GF(2^4)$ 上の乗算の結線表現（結線パターン）を、 $GF(2^4)$ の1～Fの元の各々について示す。なお、前述したように、結合部分では、排他的論理和がなされる。

【0201】

上記した基準を満たす構成の大MDSを作成する場合には、図30～図34における16個の結線部分を、図38の3, 6, C, B, 5, A, 7, Eに対応する結線表現（結線パターン）のうちから適宜選択して組み合わせて構成することができる。ただし、その逆変換に対応する構成についても、同様の条件が満たされていることが必要である。

【0202】

また、この場合に、暗号側の大MDS（の候補）を決めた場合の復号側の大MDS（の候補）、または逆に復号側の大MDS（の候補）を決めた場合の暗号側の大MDS（の候補）は、図37(b)のような行列の逆行列を求めることに

よって、容易に得られる。

【0203】

つまり、 $GF(2^4)$ による行列とその逆行列の全ての要素が 3, 6, C, B, 5, A, 7, E のいずれかであれば、上記した基準を満たすことになる。

【0204】

ここで、上記した基準を満たす MDS 行列表現を、図 39 (a) ~ (d)、図 40 (a) ~ (d) に例示する。

【0205】

なお、これら行列の探索は、次の制約の下で行ったものである。

(一) 行列は巡回型とする。

(二) 要素を並べ替えて一致するものは 1 個だけ選ぶ。

ここで、並べ替えは、巡回 $(1, 2, 3, 4) \rightarrow (2, 3, 4, 1)$ と、反転 $(1, 2, 3, 4) \rightarrow (4, 3, 2, 1)$ を任意の回数組み合わせてできる操作とする。例えば、 $(3, 3, 7, C) \rightarrow (3, 7, C, 3) \rightarrow (3, C, 7, 3)$ は該当するが、 $(3, 3, 7, C) \rightarrow (3, 7, 3, C)$ は該当しない。

また、逆関数の関係にある行列同士を比較すると分かるように、各々の行列は、他の行列の逆行列に並べ替えを行ったものになっている。例えば、 $(6, B, E, E)$ は、 $(5, 5, A, E)^{-1} = (B, E, E, 6)$ を並べ替えたものになっている。

【0206】

これら線形拡散は、上記のように対応する乗算の結線表現を用いて図 30 ~ 図 34 のようにして実回路によって実現することも、行列演算または入出力変換表によっても実現することも可能である。

【0207】

図 39 (a) と (b) とは、逆関数の関係にあり、それらの一方を暗号側に用い、他方を復号側に用いればよく、この点は、図 39 (c) と (d)、図 40 (a) と (b)、図 40 (c) と (d) のそれぞれについても、同様である（なお、暗号側と復号側とで、どのような実現方法を採用するかについては、必ずしも揃える必要はない（もちろん、揃えてもよい））。

【0208】

ところで、各 $s - box$ 間の結線パターンは、図38の3, 6, C, B, 5, A, 7, Eに対応するものに限定されず、適宜設定することが可能である。例えば、図42(c)や(d)に示すような結線パターンは図38には含まれていないが、これらも使用することが可能である（なお、前述したように、該結線パターンの結合部分では、排他的論理和がなされる）。

【0209】

この場合には、図37(a)の $X_{11} \sim X_{14}$ 、 $X_{21} \sim X_{24}$ 、 $X_{31} \sim X_{34}$ 、 $X_{41} \sim X_{44}$ を16個の入力とし、 $Y_{11} \sim Y_{14}$ 、 $Y_{21} \sim Y_{24}$ 、 $Y_{31} \sim Y_{34}$ 、 $Y_{41} \sim Y_{44}$ を16個の出力として、16行16列のMDS行列を用いればよい。

【0210】

例えば、図37(b)の線形拡散は、図42のように表現することができる。すなわち、図37(b)の5、AまたはEの要素をそれぞれ対応する4行4列の行列で表現して対応する部分に入れると、図42のようになる（図42では、4行4列の部分ごとに区切って記述している）。

【0211】

そこで、例えば、ある $s - box$ 間の結線パターンとして図42(c)あるいは(d)に示すような結線パターンを用いる場合には、図38のような16行16列の行列の対応する4行4列の部分を、図42(c)あるいは(d)に示すような4行4列表現に設定すればよい。他の所望の結線パターンを用いる場合も同様である。なお、結線パターンの4行4列表現は、当該結線パターンの入力側を4つの1ビット入力と、出力側を4つの1ビット出力として考えた場合の変換行列となっているものである。

【0212】

このように図30～図33の $s - box$ 間の結線パターンとして任意の結線パターンを用いる場合にも、暗号側について図42のように表現した場合の行列の逆行列が、復号側について図42のように表現した場合の行列となる。また、この場合の線形拡散も、任意の結線パターンを用いて（図30～図34と同様に）実回路によって実現することも、行列演算または入出力変換表によっても実

現することも可能である。

【0 2 1 3】

ところで、上記では基準 (1) として、

(1) 前段の拡大 $S - box$ の前半における全 $S - box$ のうちから任意に選んだ1つの $S - box$ と、後段の拡大 $S - box$ の前半における全 $S - box$ のうちから任意に選んだ1つの $S - box$ とが、いずれもの組み合わせについても、2本以上の経路によって相互に接続 (結合) されている。

としたが、

この条件を緩和して構成することも可能である。

【0 2 1 4】

例えば、次の条件が考えられる。

(1') 前段の拡大 $S - box$ と後段の拡大 $S - box$ との全ての組み合わせの各々において、少なくとも1組の、当該前段の拡大 $S - box$ の後半の4つの $s - box$ のうちの1つと当該後段の拡大 $S - box$ の前半の4つの $s - box$ のうちの1つとが、2本以上の経路によって相互に接続 (結合) されている。

また、例えば、次の条件が考えられる。

(1'') 前段の拡大 $S - box$ の前半における少なくとも1つの $S - box$ と、後段の拡大 $S - box$ の前半における少なくとも1つの $S - box$ とが、2本以上の経路によって相互に接続 (結合) されている。

【0 2 1 5】

このような条件の場合には、 $S - box$ 間の結線パターンを $GF(2^4)$ 上の乗算の結線表現 (結線パターン) に限定するときでも、図 3 8 の 1 ~ F に対応する結線表現 (結線パターン) のうちから適宜選択して組み合わせて構成することができる。

【0 2 1 6】

また、 $S - box$ 間の結線パターンを $GF(2^4)$ 上の乗算の結線表現 (結線パターン) に限定しないときは、例えば図 4 2 (a) や (b) に例示するものをはじめ様々な結線パターンあるいは対応する行列を用いることができる。

【0 2 1 7】

なお、以上では、暗号側と復号側で同一の基準を適用するものとしたが、暗号側と復号側で異なる基準を採用することも可能である。例えば、暗号側と復号側の一方には上記基準（１）を適用し、他方には上記基準（１'）を適用することも可能である。また、その他の適用の仕方も可能である。

【0218】

なお、上記と同様の考え方により、８ビット・データのうちの同じ位置の２ビットごとに処理を行うこととして、各要素が８ビットの４行４列のMDS行列（ $GF(2^8)$ ）を、４個用意して、大MDSを構成することも可能である。また、８ビット・データのうちの同じ位置の４ビットごとに処理を行うこととして、各要素が１６ビットの４行４列のMDS行列（ $GF(2^{16})$ ）を、２個用意して、大MDSを構成することも可能である。また、各要素が３２ビットの４行４列のMDS行列（ $GF(2^{32})$ ）を、１個用意して、大MDSを構成することも可能である。

【0219】

また、以上では、同じ位置のビットを取り出して処理を行うものとして説明したが、異なる位置のビットを（排他的に）取り出して処理を行うことも可能である。

【0220】

図４３に、大MDSの選択手順の一例を示す。

【0221】

ここでは、先に暗号側の構成を求めるものとして説明するが、その逆もちろん可能である（暗号側と復号側が逆になるだけである）。

【0222】

まず、ステップS101で、所定の方法で（例えばランダムに）、暗号側のMDS行列を求め、ステップS102で、該行列が一定の基準（例えば、前述した基準（１））を満たしているか否か判定する。一定の基準を満たしていなければ、該行列を破棄し、ステップS101で他の行列を求める。

【0223】

一定の基準を満たした場合には、ステップS103で、上記MDS行列の逆行

列すなわち復号側のMDS行列を求め、ステップS104で、該行列が一定の基準（例えば、前述した基準（1））を満たしているか否か判定する。一定の基準を満たしていなければ、これら行列を破棄し、ステップS101で他の行列を求める。

【0224】

一定の基準を満たした場合には、暗号側のMDS行列および復号側のMDS行列の組みの候補となる。

【0225】

以上の手順を繰り返し行って得た複数の候補のうちから所定の方法で選択したものを採用しても良いし、最初に得られた候補を採用するようにしてもよい。

【0226】

なお、大MDSを実回路で実現する場合には、得られたMDS行列と等価な結線パターンを用いればよい。

【0227】

なお、以上のバリエーションとして、各々の大MDSの前段及び又は後段に、同一の拡大S-boxに属する複数のS-boxについてのビットの位置を入れ替える処理を行う（あるいはそのような回路を挿入する）構成も可能である。

【0228】

もちろん、ここで説明した大MDSの構成は、これまで説明してきた種々のバリエーションを持つ暗号化装置や復号装置に適用可能である。

【0229】

例えば、上記では、1つの拡張S-boxを4並列2段分の8ビットS-boxと小MDS（と鍵加算）で構成し、このような拡張S-boxを4並列にし、4並列の拡張S-boxと大MDSとを交互に配置した（4並列の拡張S-boxと4並列の拡張S-boxとを大MDSで結合した）128ビット・ブロック暗号の暗号化装置／復号装置もしくは暗号アルゴリズム／復号アルゴリズムの場合を例にとって説明したが、もちろん、ここで説明した大MDSの構成は、上記と同様の拡張S-boxを2並列にし、2並列の拡張S-boxと大MDSとを交互に配置した（2並列の拡張S-boxと2並列の拡張S-boxとを大MD

Sで結合した) 64ビット・ブロック暗号の暗号化装置／復号装置もしくは暗号アルゴリズム／復号アルゴリズムの場合にも適用可能である。

【0230】

なお、このような64ビット・ブロック暗号の場合、128ビット・ブロック暗号の構成における4並列の拡張S-boxの部分で2並列の拡張S-boxに置き換えるとともに、これに対応する部分を修正すればよい。

【0231】

例えば、鍵長は、128ビットとすればよいし、もちろん、64ビットや96ビットなど、他の鍵長も可能である。なお、この場合の段数Rは、好ましくは6段以上とする。

【0232】

64ビット・ブロック暗号の場合、図30～図34の構成では、4並列の拡張S-boxが2並列の拡張S-boxになる点異なるが、前述した基準や結合の方法や結合パターンは同様である。また、図37(b)や図39や図40の大MDS行列は、2行2列になる。また、これに対応して、図41の大MDS行列は、8行8列になる。なお、拡張S-boxの内部構成は同じであるので、図38や図42などの結合パターンは同じものが使用可能である。また、図43の手順も同様である。

【0233】

ブロックデータがその他のデータ長の場合ももちろん可能である。

【0234】

また、拡張S-box内のS-boxの並列数が異なる場合ももちろん可能である。

【0235】

上記のような大MDSを用いた128ビット暗号の場合の一構成例に係る共通鍵ブロック暗号方式による暗号化装置あるいは復号装置は、例えば、初段では入力された128ビットの平文ブロックデータを、2段目以降では前段での処理が施された128ビットのブロックデータを入力とし、該ブロックデータを4分割した4組の32ビット・データに対してそれぞれ局所的な線形拡散処理および非

線形変換処理を施し出力する4つの第1の非線形変換処理部と、これら4つの第1の非線形変換処理部からそれぞれ出力された4組の32ビット・データを連結した128ビットのブロックデータに対して最大距離分離行列を用いて線形拡散処理を施し次段へ出力する第1の拡散処理部とを、1段分の段構成として、該段構成を所定段数分接続し、最後の前記第1の拡散処理部の後段に、この第1の拡散処理部から出力される128ビットのブロックデータを入力とする前記4つの第1の非線形変換処理部を接続し、この4つの第1の非線形変換処理部の後段に、これら4つの第1の非線形変換処理部からそれぞれ出力された4組の32ビット・データを連結した128ビットのブロックデータに対して128ビットの鍵データを加算して128ビットの暗号化されたブロックデータとして出力する第1の鍵加算部を接続して構成されるとともに、前記第1の非線形変換処理部の各々は、与えられた1組の前記32ビット・データをさらに4分割した4組の8ビット・データに対してそれぞれ8ビットの鍵データを加算する4つの第2の鍵加算部と、各第2の鍵加算部の出力に対してそれぞれ8ビットの入出力変換表を用いて非線形変換を行う4つの第2の非線形変換処理部と、これら4つの第2の非線形変換処理部からそれぞれ出力された4組の8ビット・データを連結した32ビット・データに対して最大距離分離行列を用いて線形拡散処理を施す第2の拡散処理部と、この第2の拡散処理部の後段にさらに接続された4組の前記第2の鍵加算部および第2の非線形変換処理部とを含むものであり、前記第1の拡散処理部の各々は、前段の1つの第1の非線形変換処理部の4つの第2の非線形変換処理部からそれぞれ出力される8ビットのうちの相対応する1ビットを一纏めにした4ビットを行列演算における入力側の1つの要素とするとともに、後段の1つの第1の非線形変換処理部の4つの第2の非線形変換処理部へそれぞれ入力される8ビットのうちの相対応する1ビットを一纏めにした4ビットを行列演算における出力側の1つの要素として、 2^4 のガロア体の乗算に基づいた4行4列の行列演算またはこれと等価な回路によって線形拡散処理を行う16ビット拡散手段を、該前段及び後段の第2の非線形変換処理部についての該8ビットのうちの各ビットに対応して有し、1つの前記16ビット拡散手段における前記 2^4 のガロア体の乗算に基づいた4行4列の行列演算またはこれと等価な回路では、前段

の4つの第1の非線形変換処理手段の最終段における合計16の第2の非線形変換処理手段からの出力となる任意の1ビットと、後段の4つの第1の非線形変換処理手段の初段における合計16の第2の非線形変換処理手段へ入力となる任意の1ビットとのすべての組み合わせにおいて、前段側における当該1ビットの状態を、後段側における当該1ビットへ、複数の演算経路を辿って波及させるための手段を含むものである。

【 0 2 3 6 】

また、上記のような大MDSを用いた64ビット暗号の場合の一構成例に係る共通鍵ブロック暗号方式による暗号化装置あるいは復号装置は、例えば、初段では入力された64ビットの平文ブロックデータを、2段目以降では前段での処理が施された64ビットのブロックデータを入力とし、該ブロックデータを2分割した2組の32ビット・データに対してそれぞれ局所的な線形拡散処理および非線形変換処理を施し出力する2つの第1の非線形変換処理部と、これら2つの第1の非線形変換処理部からそれぞれ出力された2組の32ビット・データを連結した64ビットのブロックデータに対して最大距離分離行列を用いて線形拡散処理を施し次段へ出力する第1の拡散処理部とを、1段分の段構成として、該段構成を所定段数分接続し、最後の前記第1の拡散処理部の後段に、この第1の拡散処理部から出力される64ビットのブロックデータを入力とする前記2つの第1の非線形変換処理部を接続し、この2つの第1の非線形変換処理部の後段に、これら2つの第1の非線形変換処理部からそれぞれ出力された2組の32ビット・データを連結した64ビットのブロックデータに対して64ビットの鍵データを加算して64ビットの暗号化されたブロックデータとして出力する第1の鍵加算部を接続して構成されるとともに、前記第1の非線形変換処理部の各々は、与えられた1組の前記32ビット・データをさらに4分割した4組の8ビット・データに対してそれぞれ8ビットの鍵データを加算する4つの第2の鍵加算部と、各第2の鍵加算部の出力に対してそれぞれ8ビットの入出力変換表を用いて非線形変換を行う4つの第2の非線形変換処理部と、これら4つの第2の非線形変換処理部からそれぞれ出力された4組の8ビット・データを連結した32ビット・データに対して最大距離分離行列を用いて線形拡散処理を施す第2の拡散処理部と

、この第2の拡散処理部の後段にさらに接続された4組の前記第2の鍵加算部および第2の非線形変換処理部とを含むものであり、前記第1の拡散処理部の各々は、前段の1つの第1の非線形変換処理部の4つの第2の非線形変換処理部からそれぞれ出力される8ビットのうちの相対応する1ビットを一纏めにした4ビットを行列演算における入力側の1つの要素とするとともに、後段の1つの第1の非線形変換処理部の4つの第2の非線形変換処理部へそれぞれ入力される8ビットのうちの相対応する1ビットを一纏めにした4ビットを行列演算における出力側の1つの要素として、 2^4 のガロア体の乗算に基づいた2行2列の行列演算またはこれと等価な回路によって線形拡散処理を行う8ビット拡散手段を、該前段及び後段の第2の非線形変換処理部についての該8ビットのうちの各ビットに対応して有し、1つの前記8ビット拡散手段における前記 2^4 のガロア体の乗算に基づいた2行2列の行列演算またはこれと等価な回路では、前段の2つの第1の非線形変換処理手段の最終段における合計8の第2の非線形変換処理手段からの出力となる任意の1ビットと、後段の2つの第1の非線形変換処理手段の初段における合計8の第2の非線形変換処理手段へ入力となる任意の1ビットとのすべての組み合わせにおいて、前段側における当該1ビットの状態を、後段側における当該1ビットへ、複数の演算経路を辿って波及させるための手段を含むものである。

【0237】

以下では、本実施形態のハードウェア構成、ソフトウェア構成について説明する。

【0238】

本実施形態の暗号化装置や復号装置は、ハードウェアとしても、ソフトウェアとしても、実現可能である。

【0239】

本実施形態は、ソフトウェアで実現する場合に、暗号化装置や復号装置を実現するプログラムであって、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可

能な記録媒体としても実施することもできる。

【0240】

また、ハードウェアとして構成する場合、半導体装置として形成することができる。

【0241】

また、本発明を適用した暗号化装置や復号装置を構成する場合、あるいは暗号化プログラムや復号プログラムを作成する場合に、図4や図24で例示したようなブロックもしくはモジュールをすべて個別に作成することも可能であるが、同一構成を有するブロックもしくはモジュールについては1または適当数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。

【0242】

また、ソフトウェアの場合には、マルチプロセッサを利用し、並列処理を行って、処理を高速化することも可能である。

【0243】

なお、暗号化機能を持ち、復号機能を持たない装置として構成することも、復号機能を持ち、暗号化機能を持たない装置として構成することも、暗号化機能と復号機能の両方を持つ装置として構成することも、可能である。同様に、暗号化機能を持ち、復号機能を持たないプログラムとして構成することも、復号機能を持ち、暗号化機能を持たないプログラムとして構成することも、暗号化機能と復号機能の両方を持つプログラムとして構成することも、可能である。

【0244】

次に、本実施形態のシステムへの応用について説明する。

【0245】

本実施形態の暗号方式は、基本的にはどのようなシステムにも適用可能である。

【0246】

例えば、図44に示すように、送信側装置301と、受信側装置303との間で、所定の方法もしくは手続により、鍵を安全に共有しておき、送信側装置30

1 は送信データをブロック長ごとに本実施形態の暗号方式で暗号化し、所定のプロトコルに従って、通信ネットワーク 3 0 2 を介して、暗号文を受信側装置 3 0 3 へ送信し、暗号文を受信した受信側装置 3 0 3 では、受信した暗号文をブロック長ごとに本実施形態の暗号方式で復号し、もとの平文を得ることができる。なお、各々の装置が、暗号化機能と復号機能を両方持っていれば、双方向に暗号通信を行うことができる。

【 0 2 4 7 】

また、例えば、図 4 5 に示すように、計算機 3 1 1 では、所定の方法で鍵を生成し、保存したいデータをブロック長ごとに本実施形態の暗号方式で暗号化し、所定のネットワーク（例えば、LAN、インターネット等）3 1 4 を介して、暗号化データとして、データ・サーバ 3 1 3 に保存しておく。計算機 3 1 1 では、このデータを読みたいときは、データ・サーバ 3 1 3 から所望の暗号化データを読み込み、これをブロック長ごとに本実施形態の暗号方式で復号し、もとの平文を得ることができる。また、他の計算機 3 1 2 が、この鍵を知っていれば、同様に復号してもとの平文を得ることができるが、鍵の分からない他の計算機は、該暗号データを復号することはできず、情報のセキュリティ・コントロールが可能になる。

【 0 2 4 8 】

また、例えば、図 4 6 に示すように、コンテンツ提供側では、暗号化装置 3 2 1 により、あるコンテンツを、ある鍵で、ブロック長ごとに本実施形態の暗号方式で暗号化し、これを暗号化コンテンツとして、記録媒体 3 2 2 に記録し、これを頒布等する。記録媒体 3 2 2 を取得したユーザ側では、所定の方法で該ある鍵を入手することにより、復号装置 3 2 3 により、該コンテンツを、ブロック長ごとに本実施形態の暗号方式で復号し、コンテンツの閲覧もしくは再生等を行うことができる。

【 0 2 4 9 】

もちろん、上記以外にも種々のシステムに適用可能である。

【 0 2 5 0 】

なお、本実施形態で示した各々の構成は、一例であって、それ以外の構成を排

除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。

また、各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。

また、本実施形態は、暗号化装置としての発明、復号化装置としての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。

従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【 0 2 5 1 】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【 0 2 5 2 】

【発明の効果】

本発明によれば、局所的なデータ拡散を行う小型の拡散層とブロック幅に及ぶ拡散を行う大型の拡散層を交互に重ねて運用することにより、計算コストを抑えたまま高く均一な拡散を実現することができる。

【図面の簡単な説明】

【図 1】

本発明の一実施形態に係る暗号方式の基本的な構成について説明するための図

【図 2】

同実施形態の暗号強度に関して説明するための図

【図 3】

同実施形態の入れ子型暗号方式のデータ攪拌部の階層構造の例を示す図

【図 4】

同実施形態の暗号化装置の構成例を示す図

【図 5】

同実施形態の S - b o x の一例を示す図

【図 6】

同実施形態の拡大 S - b o x の内部構成例を示す図

【図 7】

同実施形態の小 M D S の一例を示す図

【図 8】

同実施形態の大 M D S および拡大 S - b o x の構造例を示す図

【図 9】

同実施形態の大 M D S の一例を示す図

【図 1 0】

同実施形態の大 M D S の他の例を示す図

【図 1 1】

同実施形態の鍵スケジュール部の構成例を示す図

【図 1 2】

同実施形態の鍵スケジュール部の他の構成例を示す図

【図 1 3】

同実施形態の非線形変換層の内部構成の一例を示す図

【図 1 4】

同実施形態の非線形変換層の内部構成の他の例を示す図

【図 1 5】

同実施形態の加算定数表の一例を示す図

【図 1 6】

同実施形態の有限体乗算装置の構成例を示す図

【図 1 7】

同実施形態の線形変換装置の構成例を示す図

【図 1 8】

同実施形態の線形変換装置の構成例を示す図

【図 1 9】

同実施形態のMD S 行列生成装置の構成例を示す図

【図 2 0】

同実施形態のMD S 行列生成処理手順の一例を示すフローチャート

【図 2 1】

同実施形態のMD S 行列生成装置の他の構成例を示す図

【図 2 2】

同実施形態のMD S 行列生成処理手順の他の例を示すフローチャート

【図 2 3】

同実施形態の S - b o x と小MD S の組み合わせを選択するための処理手順の一例を示すフローチャート

【図 2 4】

同実施形態の復号装置の構成例を示す図

【図 2 5】

同実施形態の拡大 S - b o x の内部構成例を示す図

【図 2 6】

同実施形態の大MD S および拡大 S - b o x の構造例を示す図

【図 2 7】

同実施形態の鍵スケジュール部の構成例を示す図

【図 2 8】

同実施形態の大MD S のさらに他の例を示す図

【図 2 9】

同実施形態の大MD S のさらに他の例を示す図

【図 3 0】

同実施形態の大MD S の S - b o x 間の結線パターンの一例を示す図

【図 3 1】

同実施形態の大MD S の S - b o x 間の結線パターンの一例を示す図

【図 3 2】

同実施形態の大MDSのS - b o x間の結線パターンの一例を示す図

【図 3 3】

同実施形態の大MDSのS - b o x間の結線パターンの一例を示す図

【図 3 4】

同実施形態の大MDSのS - b o x間の結線パターンの一例を示す図

【図 3 5】

同実施形態の大MDSの前段と後段のS - b o x間の経路について説明するための図

【図 3 6】

従来の隣接する段のS - b o x間の経路について説明するための図

【図 3 7】

同実施形態の大MDSのGF (2^4) による行列表現について説明するための図

【図 3 8】

GF (2^4) 上の乗算の結線表現を示す図

【図 3 9】

ファン・インに関する基準 (1) を満たすMDS行列の例を示す図

【図 4 0】

ファン・インに関する基準 (1) を満たすMDS行列の例を示す図

【図 4 1】

同実施形態の大MDSの16行16列の行列表現について説明するための図

【図 4 2】

GF (2^4) 上の乗算の結線表現以外の結線表現の例を示す図

【図 4 3】

同実施形態の大MDS行列選択処理手順の一例を示すフローチャート

【図 4 4】

同実施形態の暗号方式を利用したシステムの一例を示す図

【図 4 5】

同実施形態の暗号方式を利用したシステムの他の例を示す図

【図 4 6】

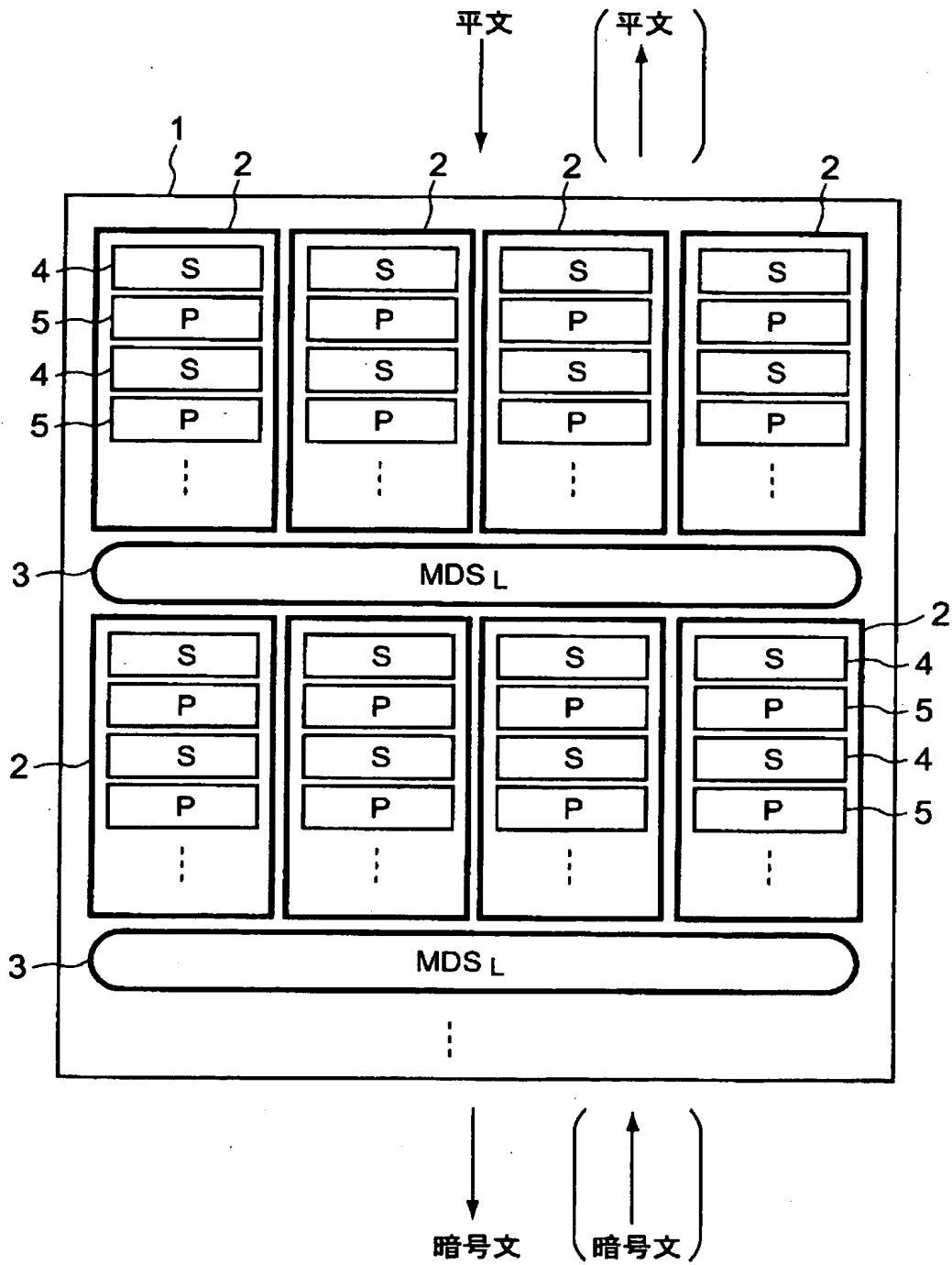
同実施形態の暗号方式を利用したシステムのさらに他の例を示す図

【符号の説明】

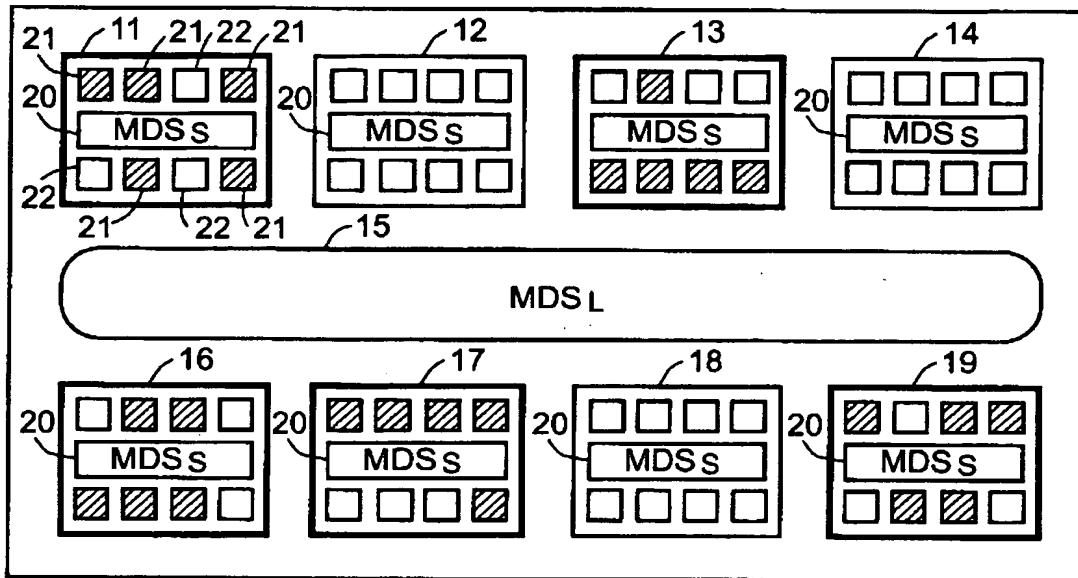
- 1 …暗号処理装置
- 2 …最上位の階層の非線形変換モジュール
- 3 …データ幅に渡る拡散モジュール
- 4 …階層構造内部の非線形変換モジュール
- 5 …局所的な拡散モジュール
- 1 0 2 …拡大 S - b o x 層
- 1 0 3, 1 1 0 3 …拡大 S - b o x
- 1 0 4, 1 3 1, 1 1 0 4 …大 M D S
- 1 0 5, 1 1 0 5 …（暗号文直前の）鍵加算部
- 1 1 1, 1 1 1 1 …鍵加算部
- 1 1 2, 1 4 1, 1 1 1 2 …S - b o x
- 1 1 3, 1 4 2, 1 1 1 3 …小 M D S
- 1 2 1 ~ 1 2 4 …鍵スケジューラ部
- 1 3 4, 1 4 3 …排他的論理和部
- 1 3 5, 1 3 6 …剰余加算部
- 2 0 0 …有限体乗算装置
- 2 0 1 …桁溢れ帰還部
- 2 0 2 …係数格納部
- 2 0 3 …乗算部
- 2 0 4, 2 0 5 …排他的論理和部
- 2 3 1 …要素生成部
- 2 3 2 …小行列式計算部
- 2 3 3 …判定部
- 2 3 4 …逆行列生成部
- 2 3 5 …逆行列判定部

【書類名】 図面

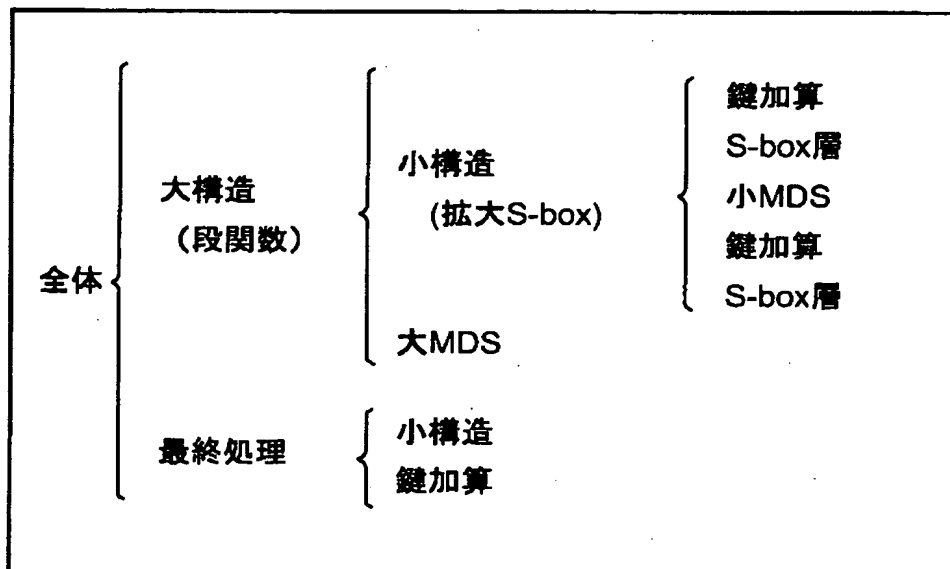
【図 1】



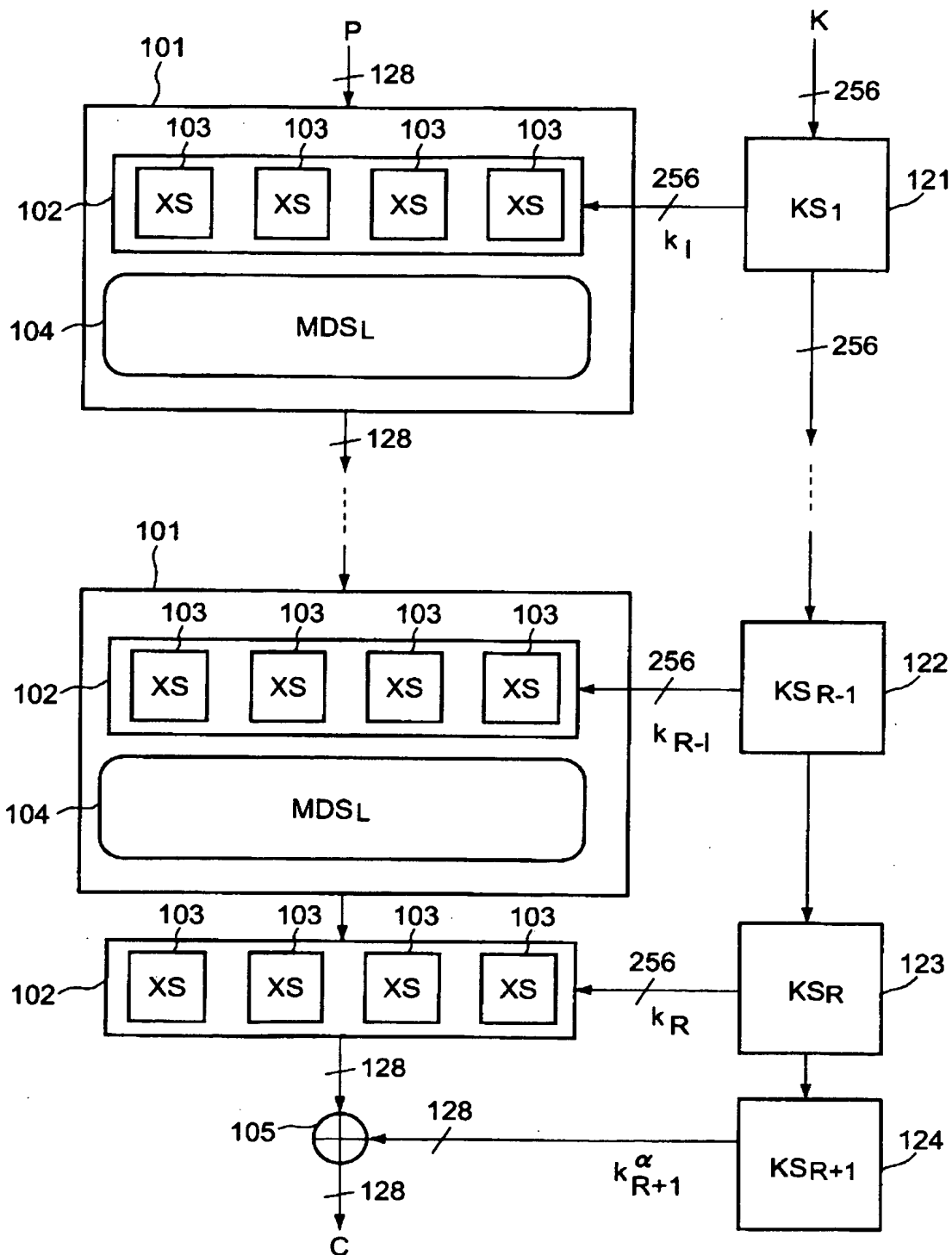
【図 2】



【図 3】



【図 4】



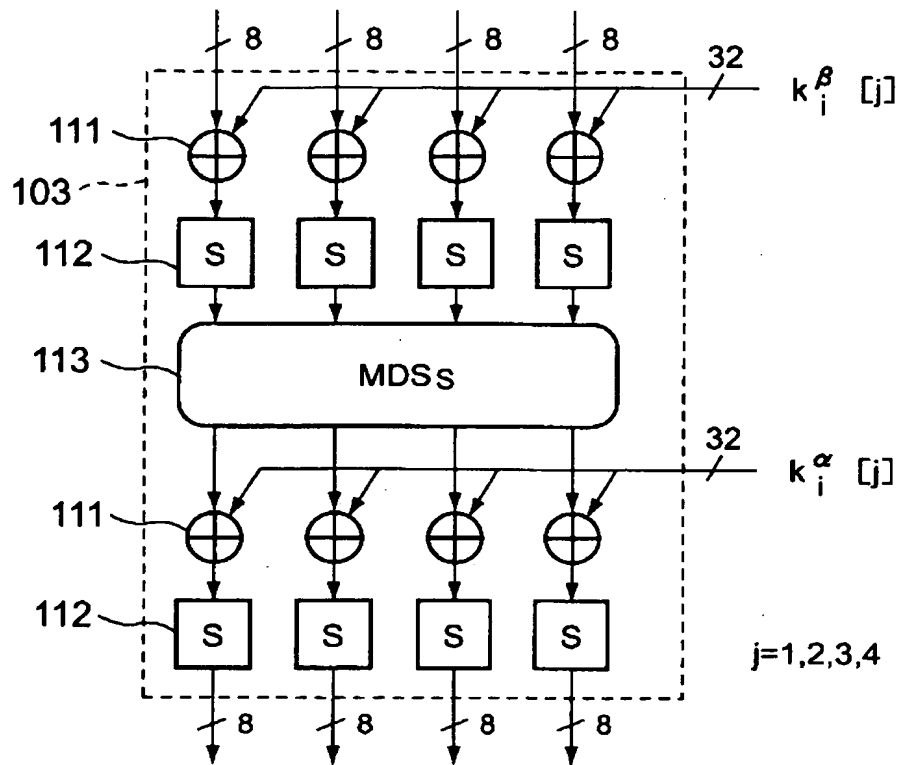
【图 5】

112

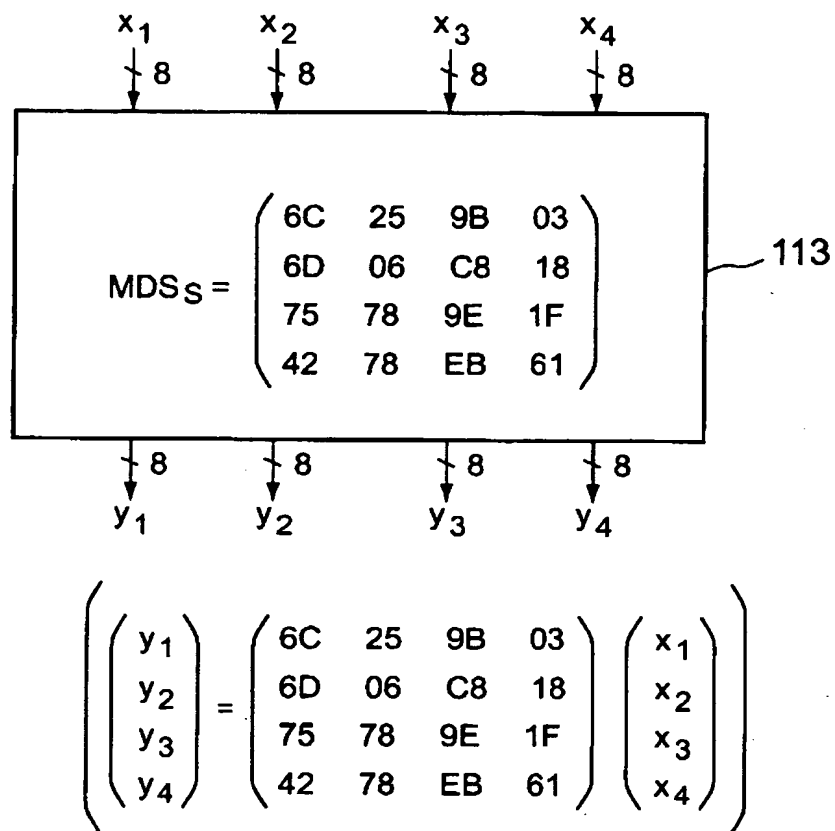
$$s[256] = \{$$

72	AA	49	16	1E	3A	43	AE	66	BC	00	73	79	3B	FB	9F
69	6A	A2	50	6E	F5	EF	AC	22	02	AD	26	E2	DF	97	F0
9E	BF	17	8B	FA	7C	F4	71	7F	CA	F6	52	FD	C3	E5	64
53	8D	E0	F3	0F	78	CB	9B	68	3C	0D	1F	89	B6	EB	F7
44	4A	06	A6	56	6B	85	01	30	88	51	31	9C	A0	A3	25
60	5B	FF	05	B7	91	15	B3	A9	20	03	2B	61	42	95	4D
F9	7E	0E	E9	D8	F1	46	99	CE	BE	D9	54	80	B0	D2	4F
7A	E8	35	92	1B	7B	12	D6	4C	D5	E7	EE	B1	24	DE	21
04	10	AB	29	9A	81	FE	A7	B8	63	28	0A	8A	D1	C6	07
B9	C8	98	82	74	9D	84	47	94	C7	6C	11	D7	BA	C1	C9
DD	77	39	2F	2E	C2	67	41	E4	58	34	CD	1C	93	96	7D
2C	F8	B5	70	14	08	DC	CC	87	D0	5E	32	C5	C4	59	3E
CF	55	5C	23	75	2D	2A	86	4B	1D	5F	E6	FC	B2	4E	09
27	AF	19	B4	BD	6D	3D	6F	ED	62	EA	F2	D3	36	38	DB
BB	83	45	37	A4	EC	8C	5D	E1	33	90	A1	40	8E	1A	A5
0B	3F	5A	DA	13	76	0C	C0	48	E3	65	A8	18	8F	D4	57

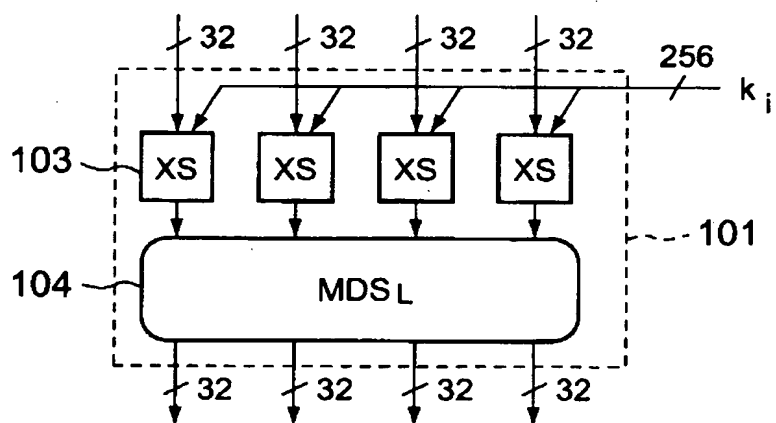
【図 6】



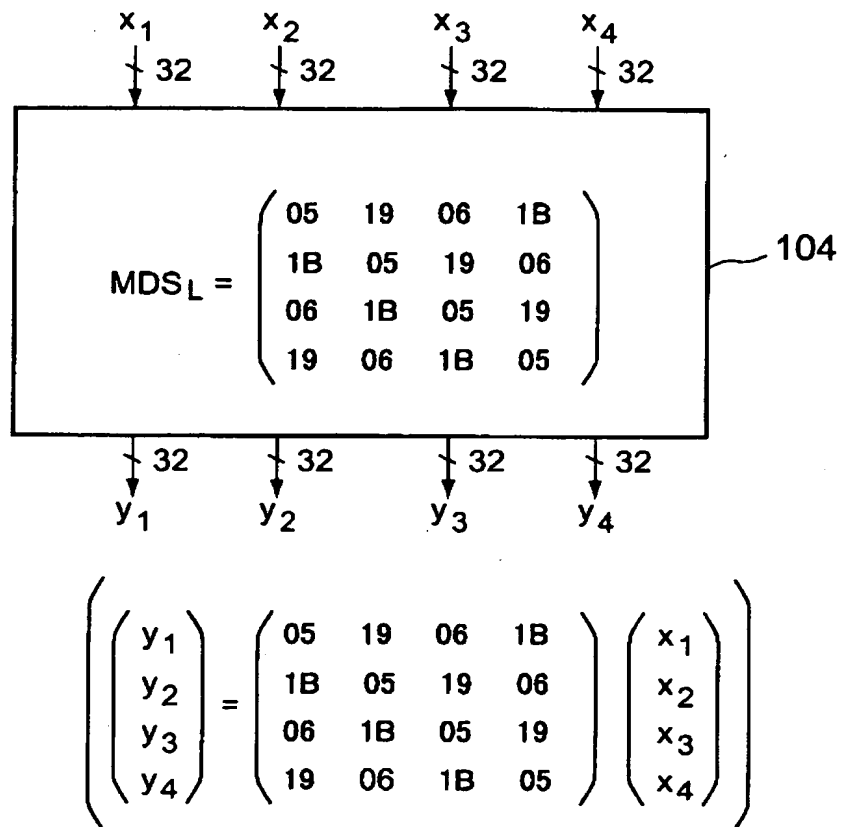
【図 7】



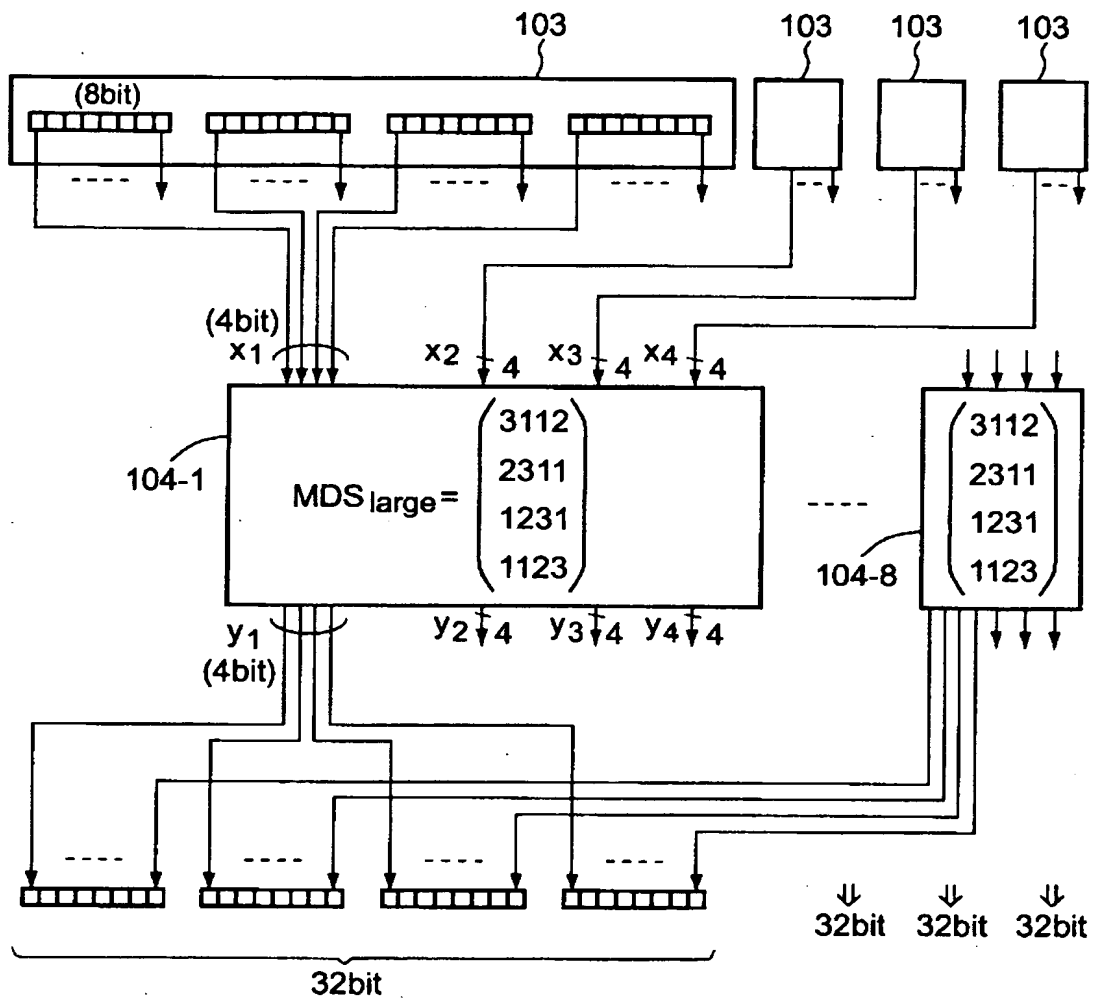
【図 8】



【図 9】

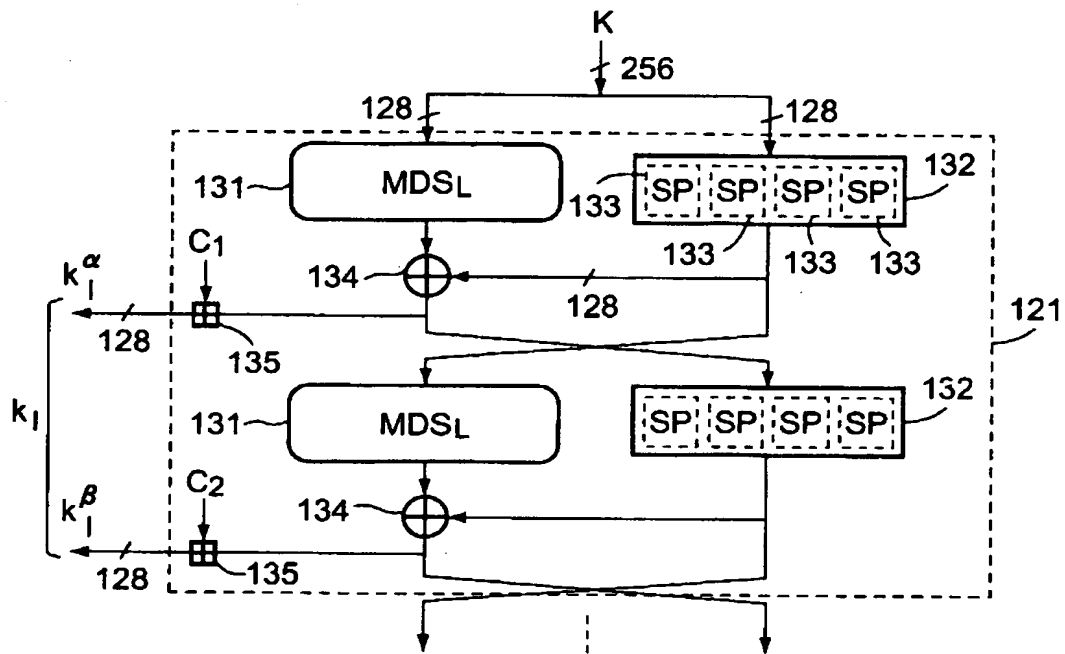


【図 1 0】

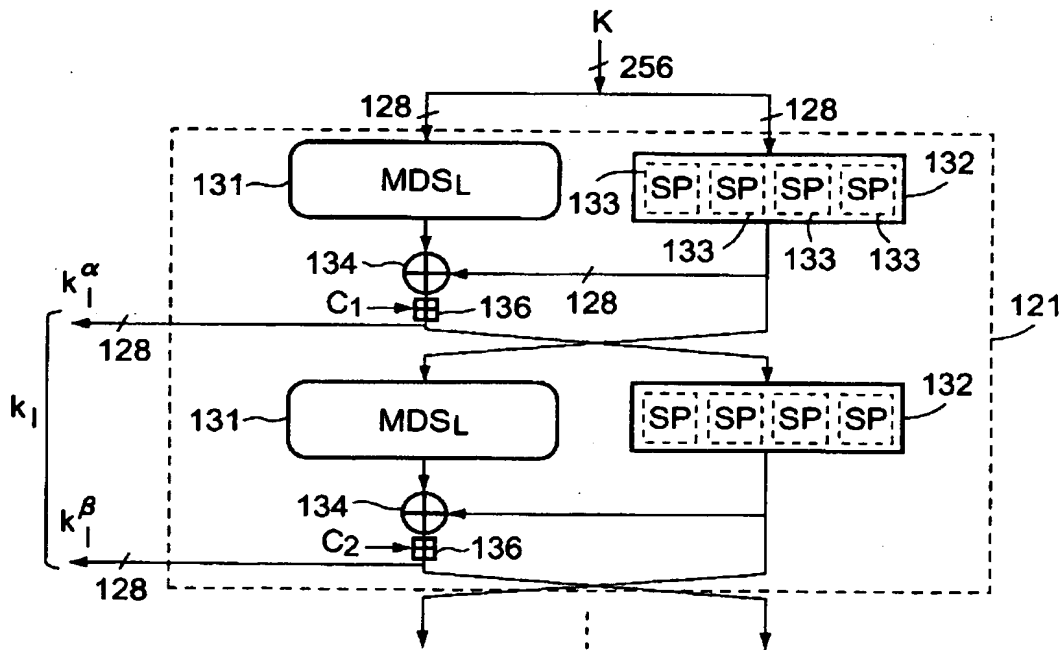


$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 3112 \\ 2311 \\ 1231 \\ 1123 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

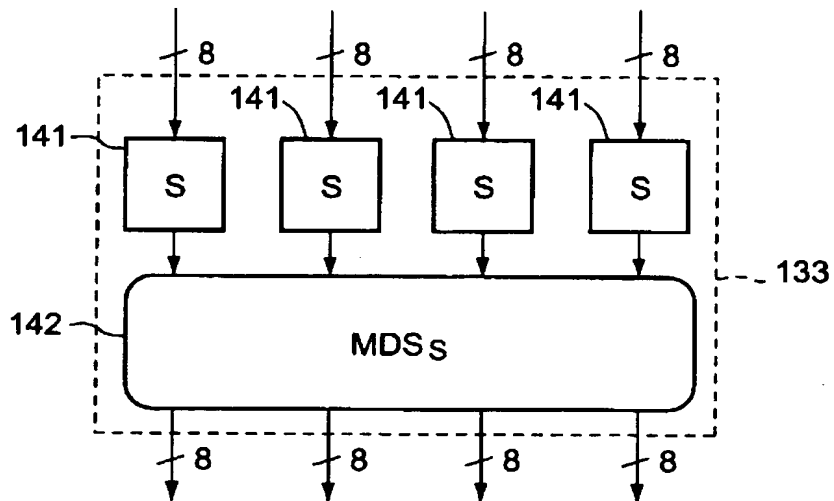
【図 1 1】



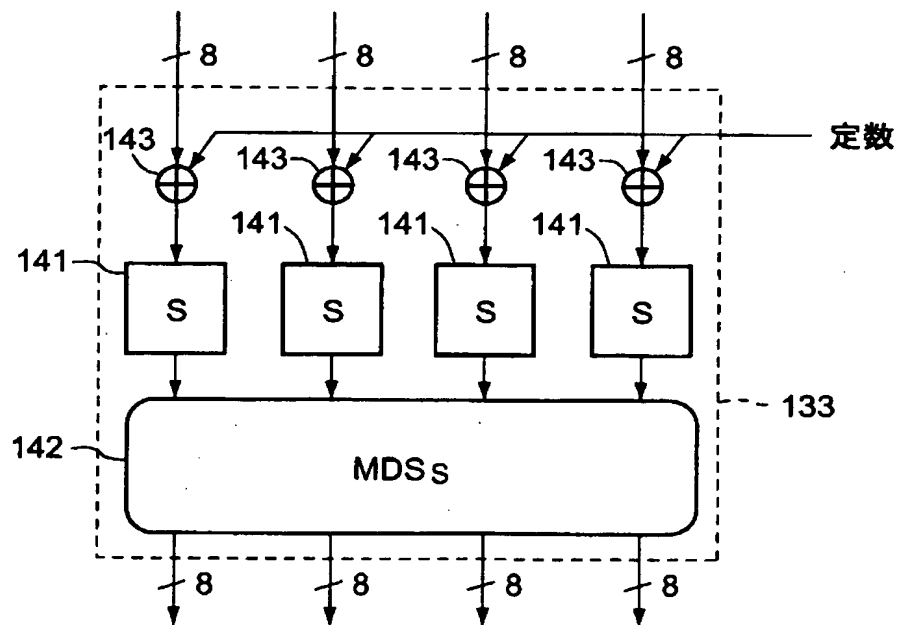
【図 1 2】



【図 1 3】



【図 1 4】



【図 1 5】

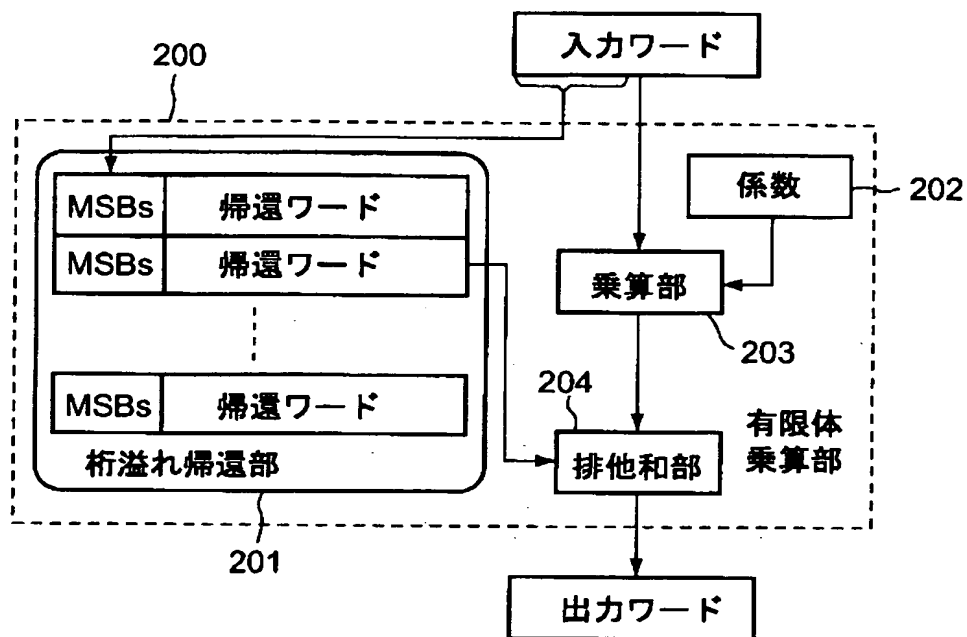
(a)

C1	(H2 ,H0 ,H1 ,H1)
C2	(H3 ,H2 ,H0 ,H3)
C3	(H1 ,H0 ,H0 ,H0)
C4	(H1 ,H0 ,H1 ,H3)
C5	(H0 ,H1 ,H0 ,H2)
C6	(H3 ,H2 ,H0 ,H0)
C7	(H1 ,H2 ,H1 ,H0)
C8	(H2 ,H1 ,H2 ,H3)
C9	(H2 ,H1 ,H0 ,H0)
C10	(H1 ,H1 ,H1 ,H2)
C11	(H3 ,H1 ,H1 ,H2)
C12	(H1 ,H1 ,H2 ,H0)
C13	(H1 ,H3 ,H3 ,H1)
C14	(H2 ,H3 ,H3 ,H1)
C15	(H1 ,H3 ,H1 ,H0)
C16	(H1 ,H0 ,H0 ,H3)
C17	(H1 ,H2 ,H0 ,H3)

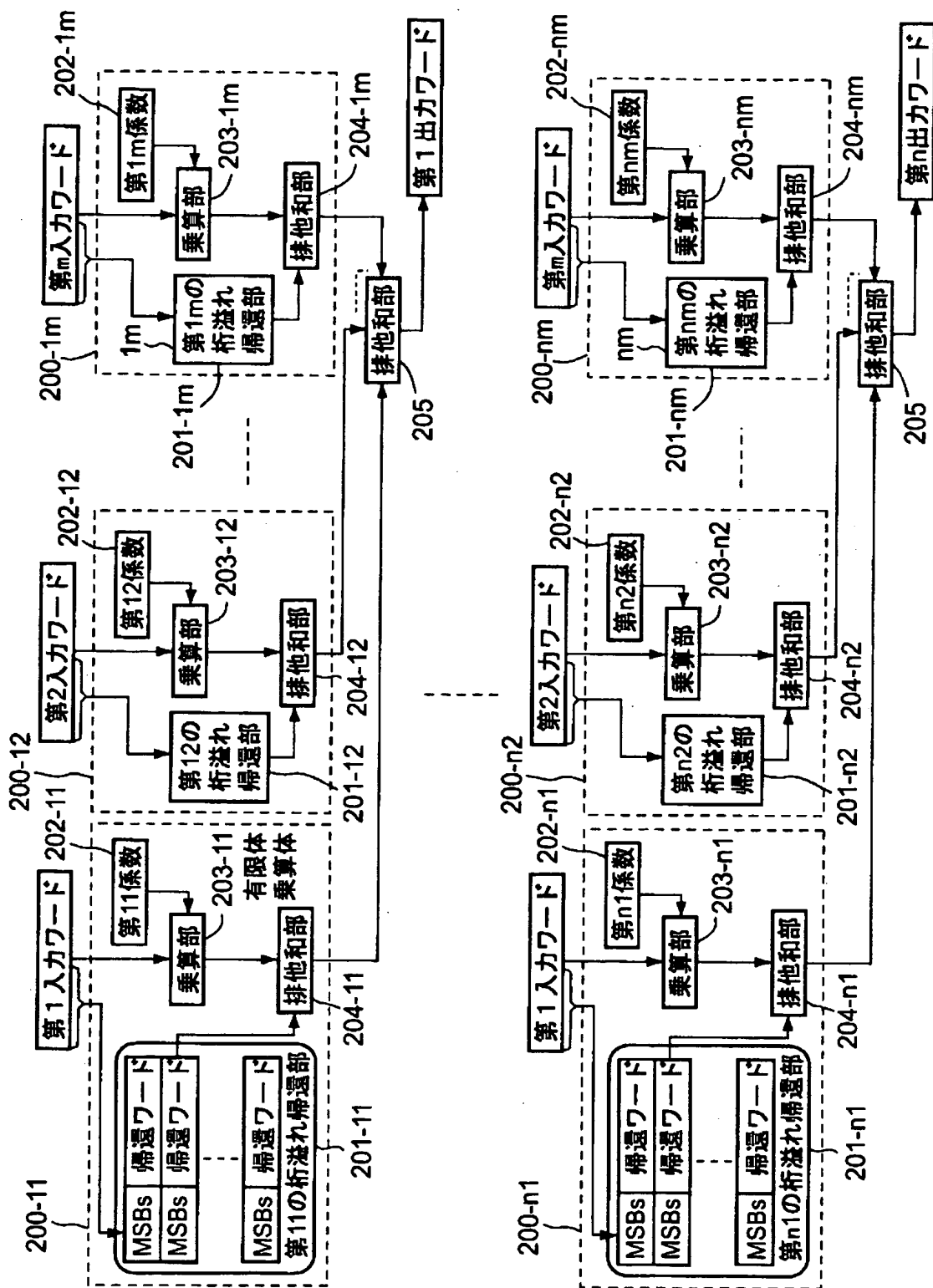
(b)

$$\left\{ \begin{array}{l} H_0 =(5a827999)_H =2^{1/2}/4 \\ H_1 =(6ed9eba1)_H =3^{1/2}/4 \\ H_2 =(8f1bbcdc)_H =5^{1/2}/4 \\ H_3 =(ca62c1d6)_H =10^{1/2}/4 \end{array} \right.$$

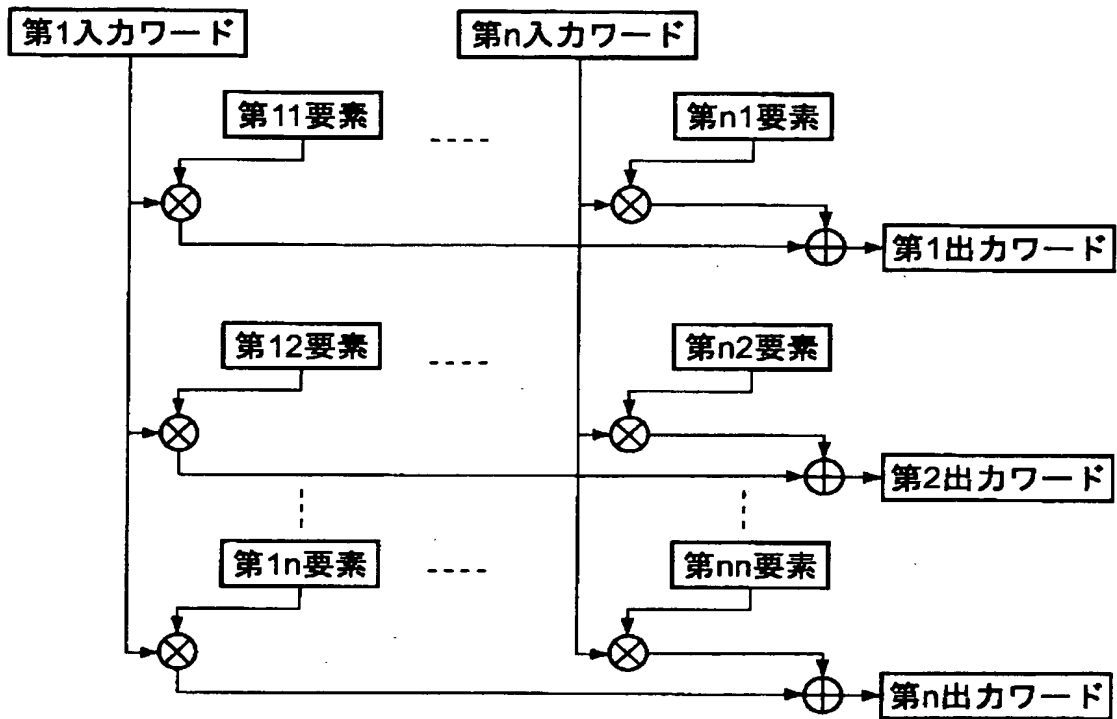
【図 1 6】



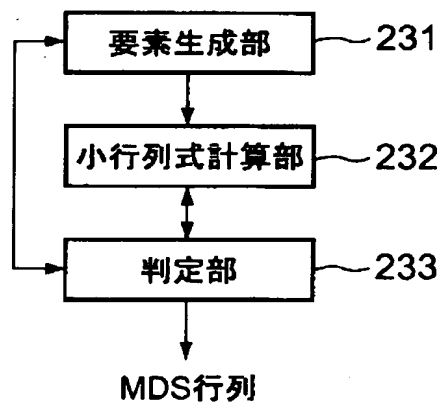
【图 1 7】



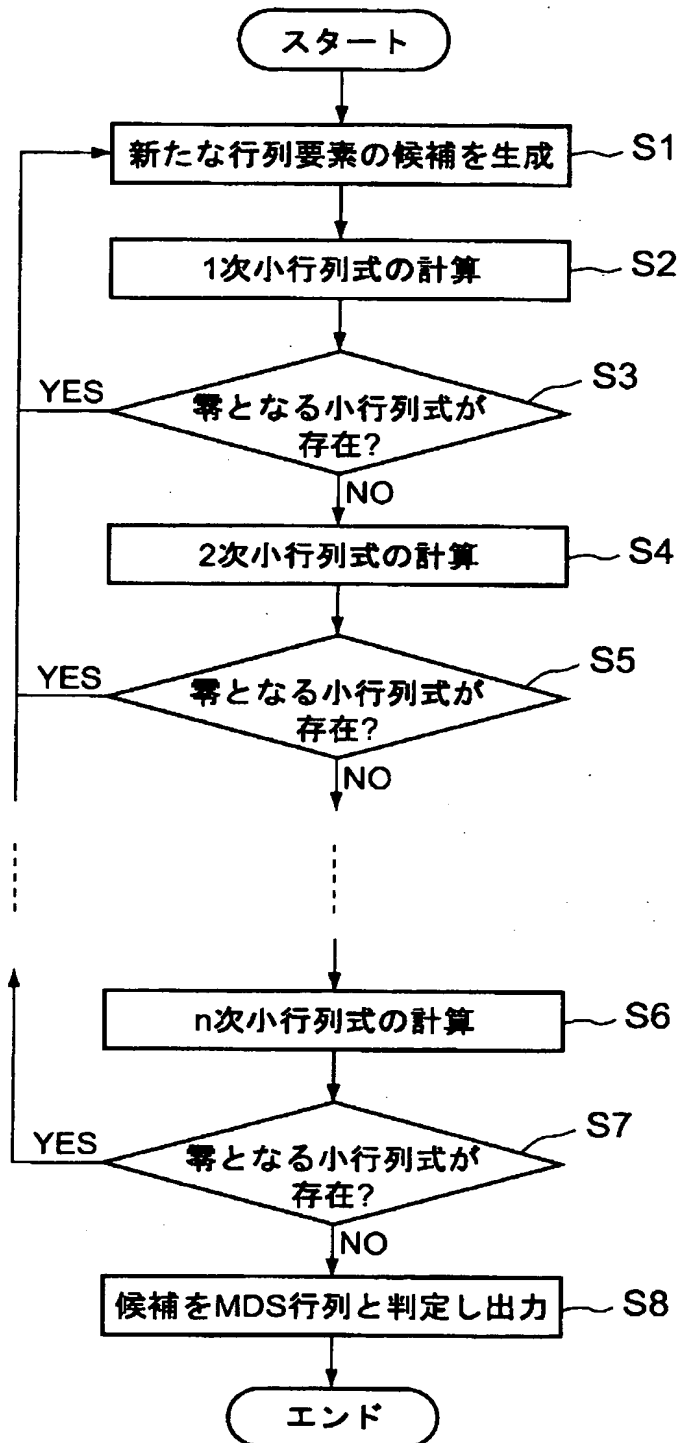
【図 1 8】



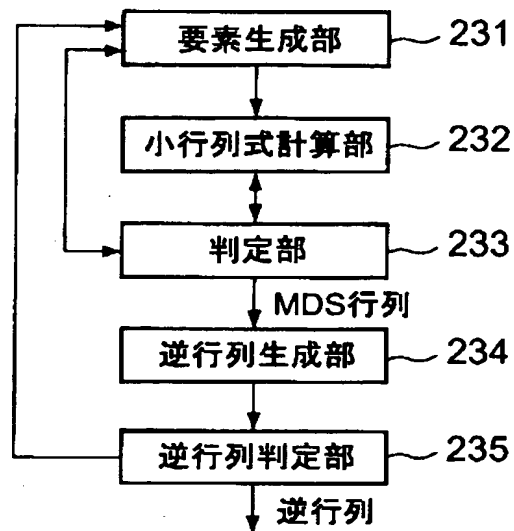
【図 1 9】



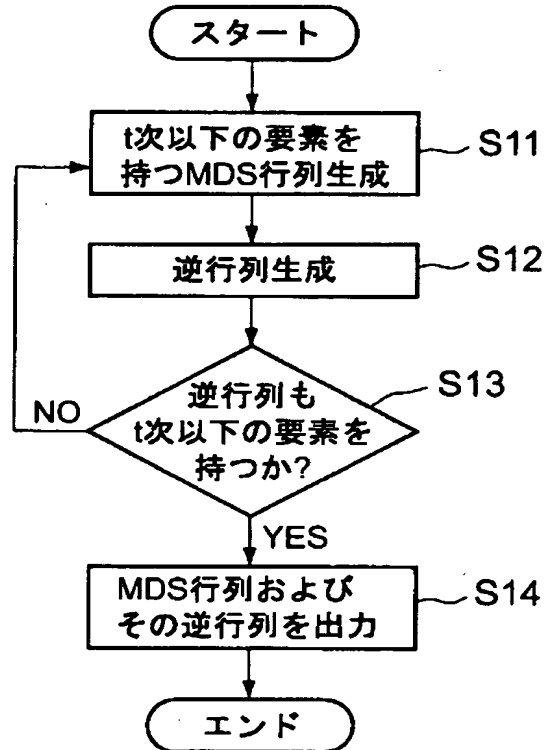
【図20】



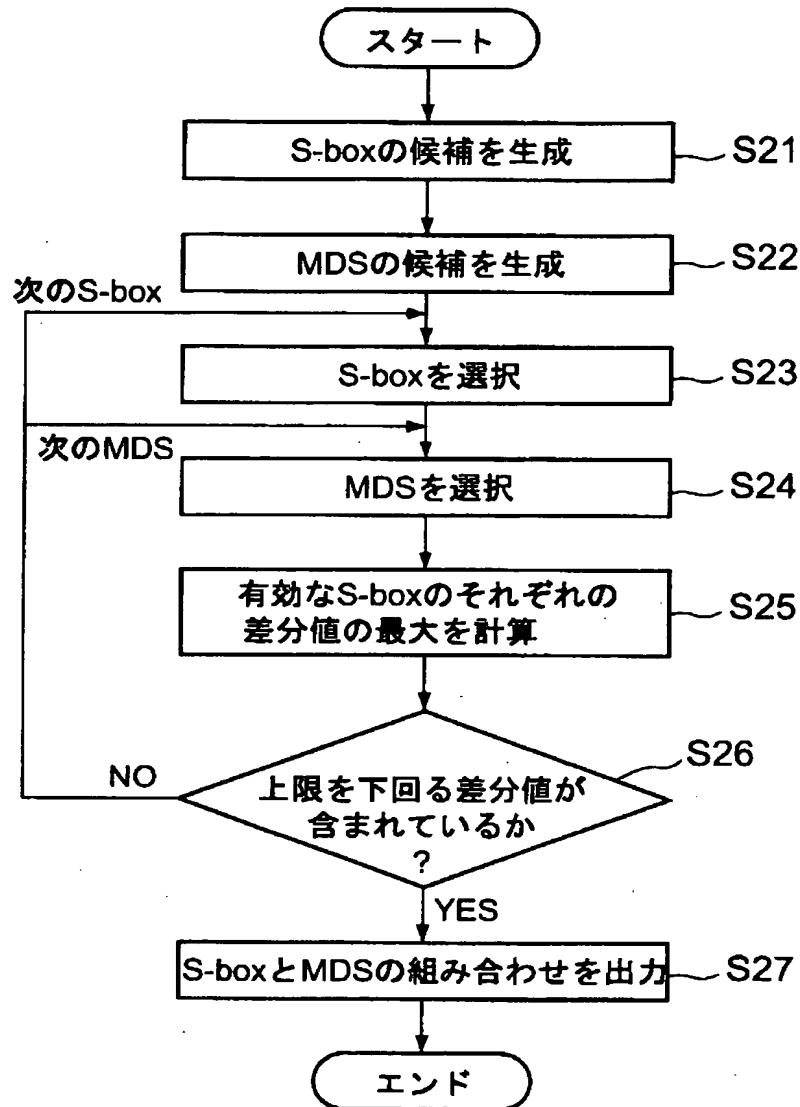
【図 2 1】



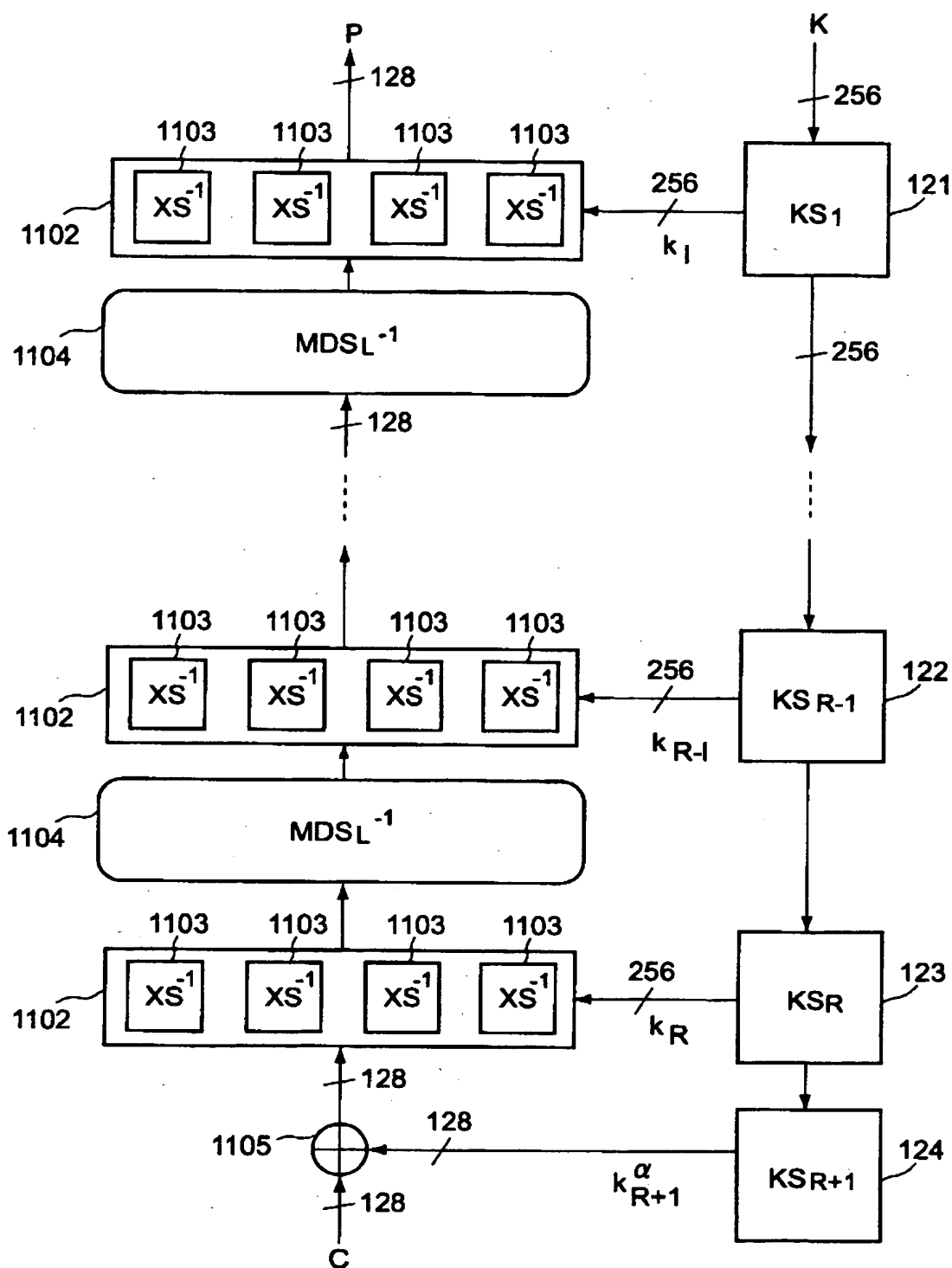
【図 2 2】



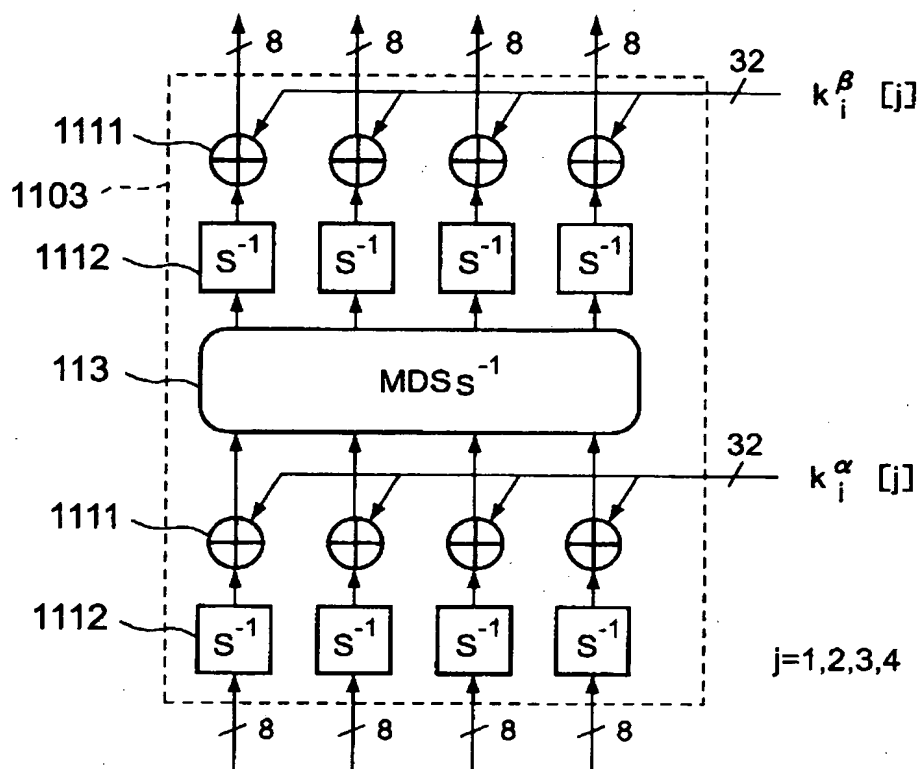
【図 2 3】



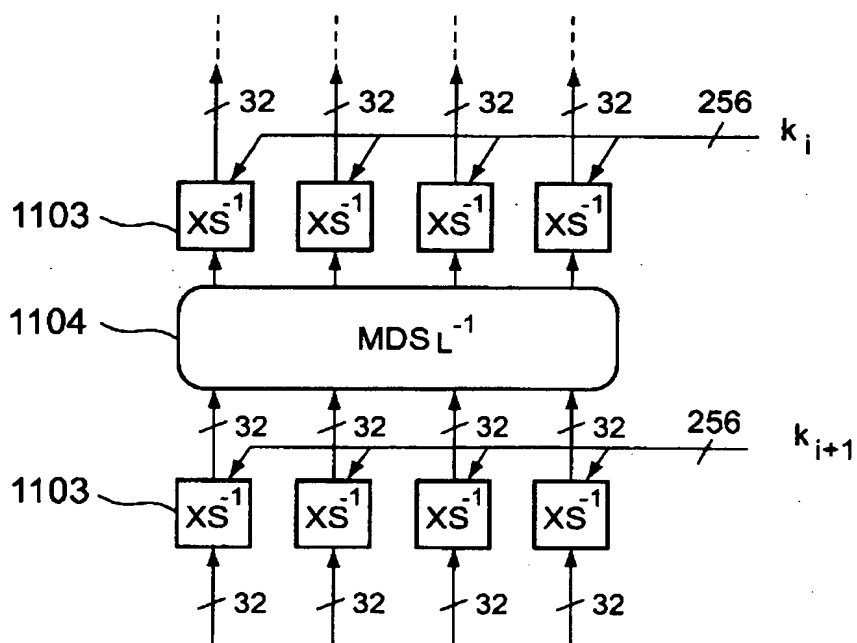
【図 24】



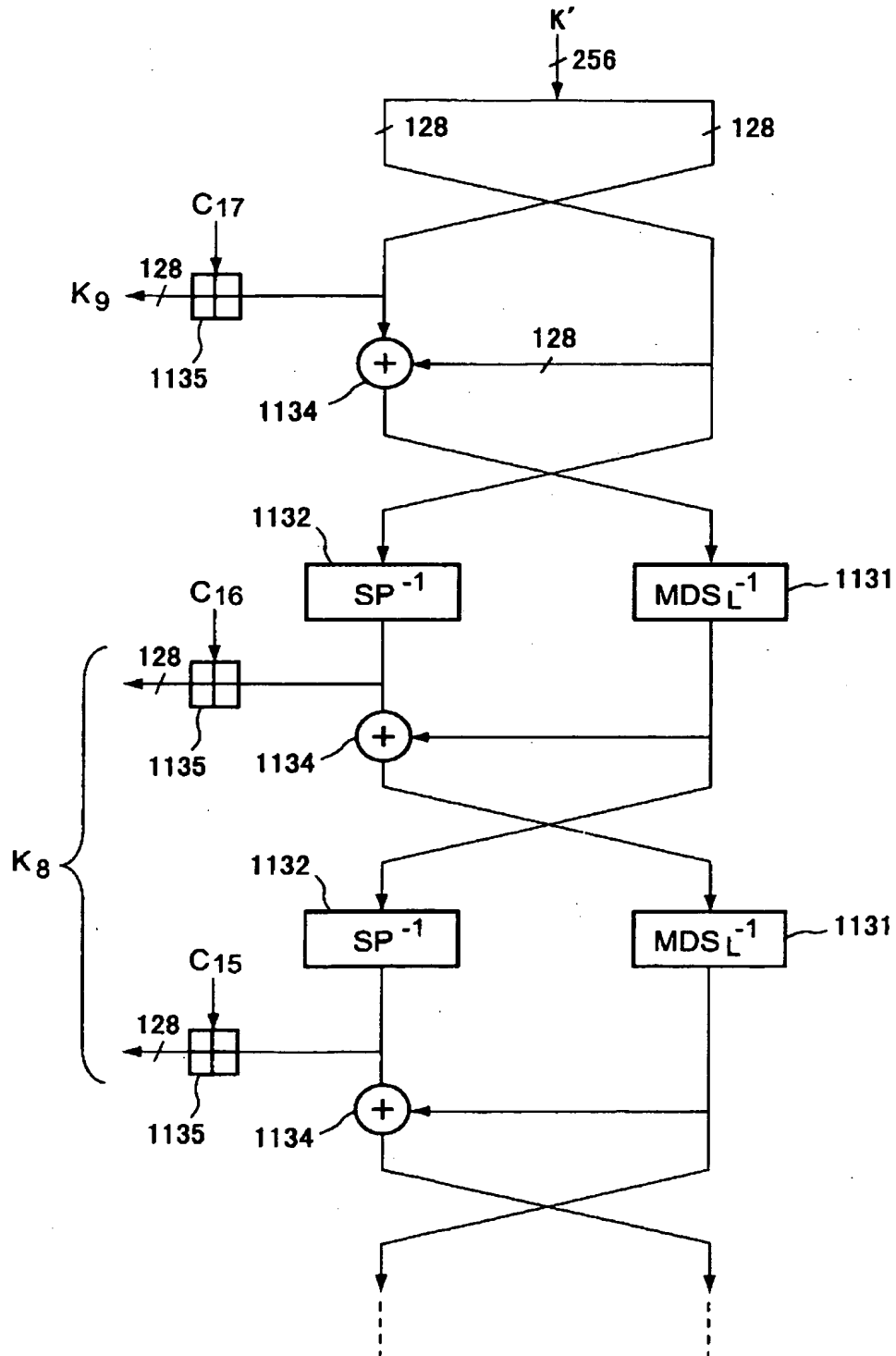
【図 25】



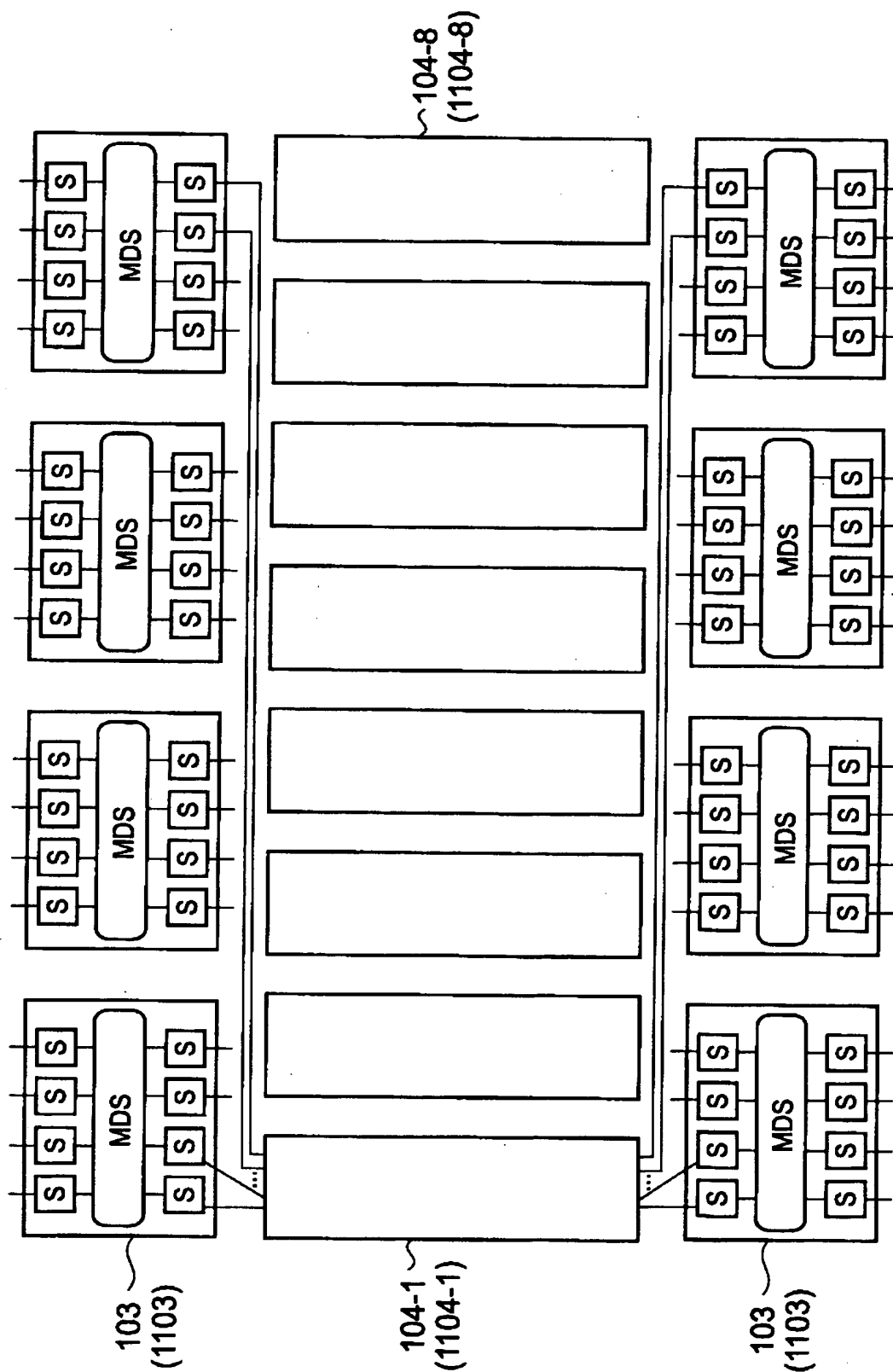
【図 26】



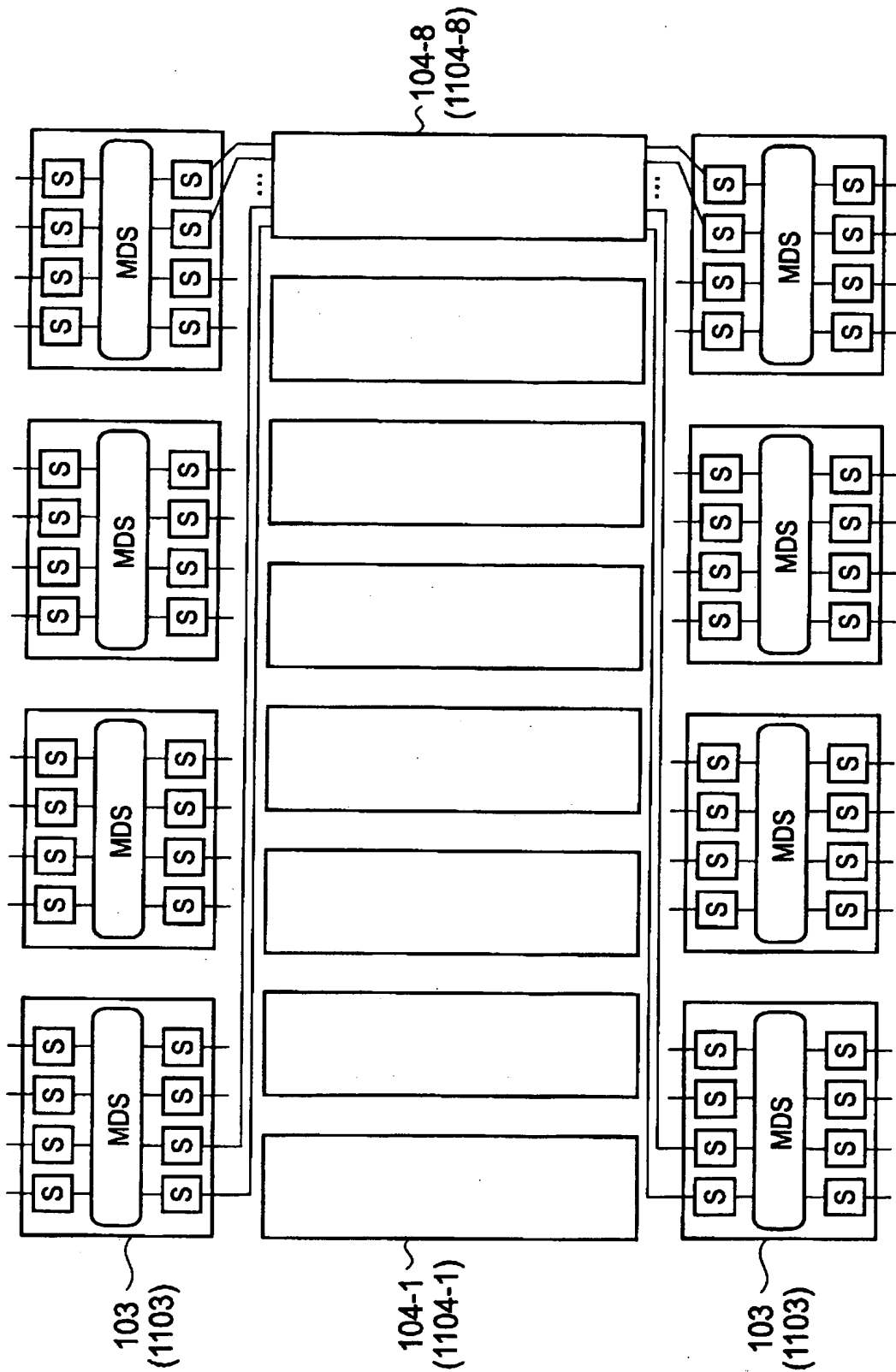
【図 27】



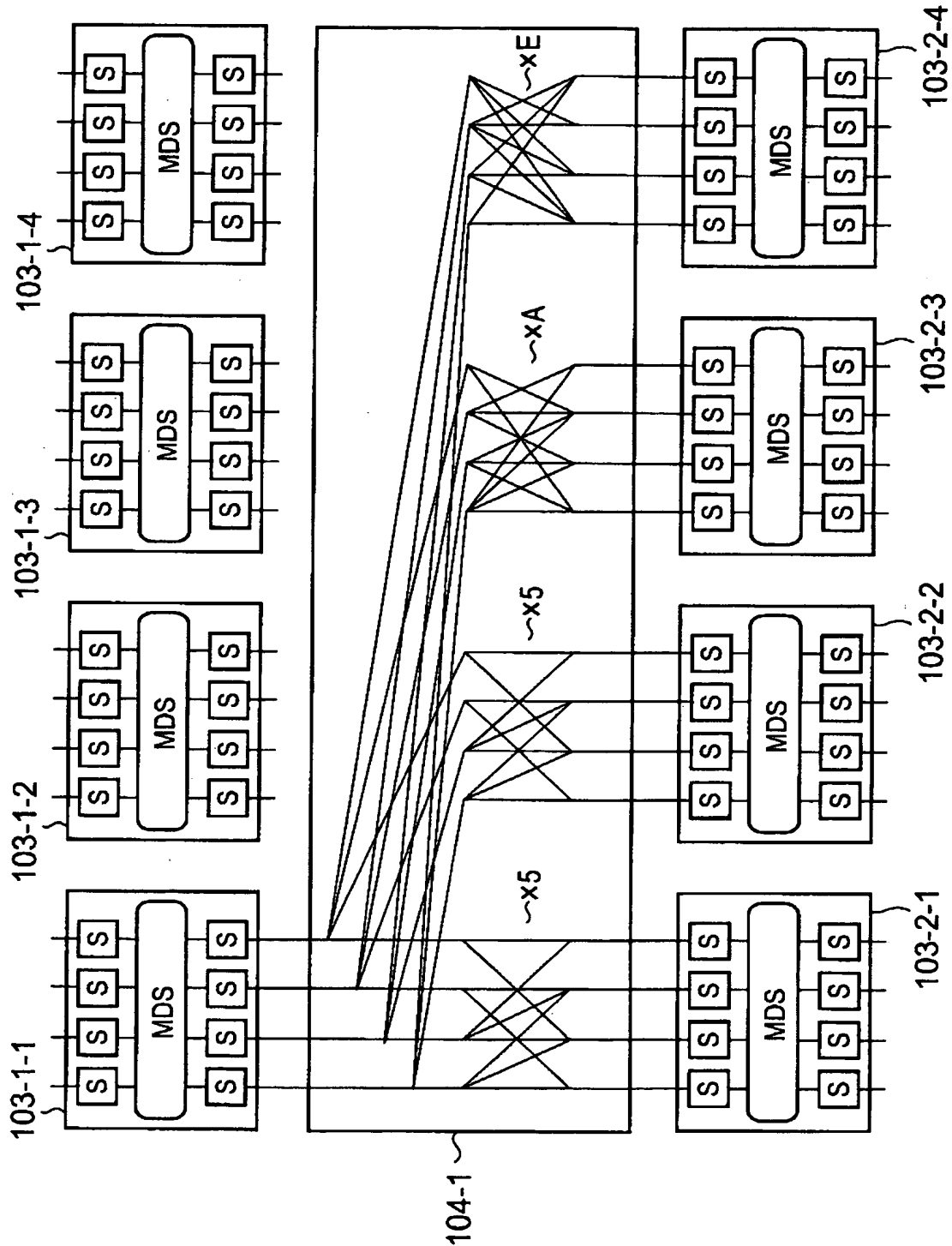
【図 28】



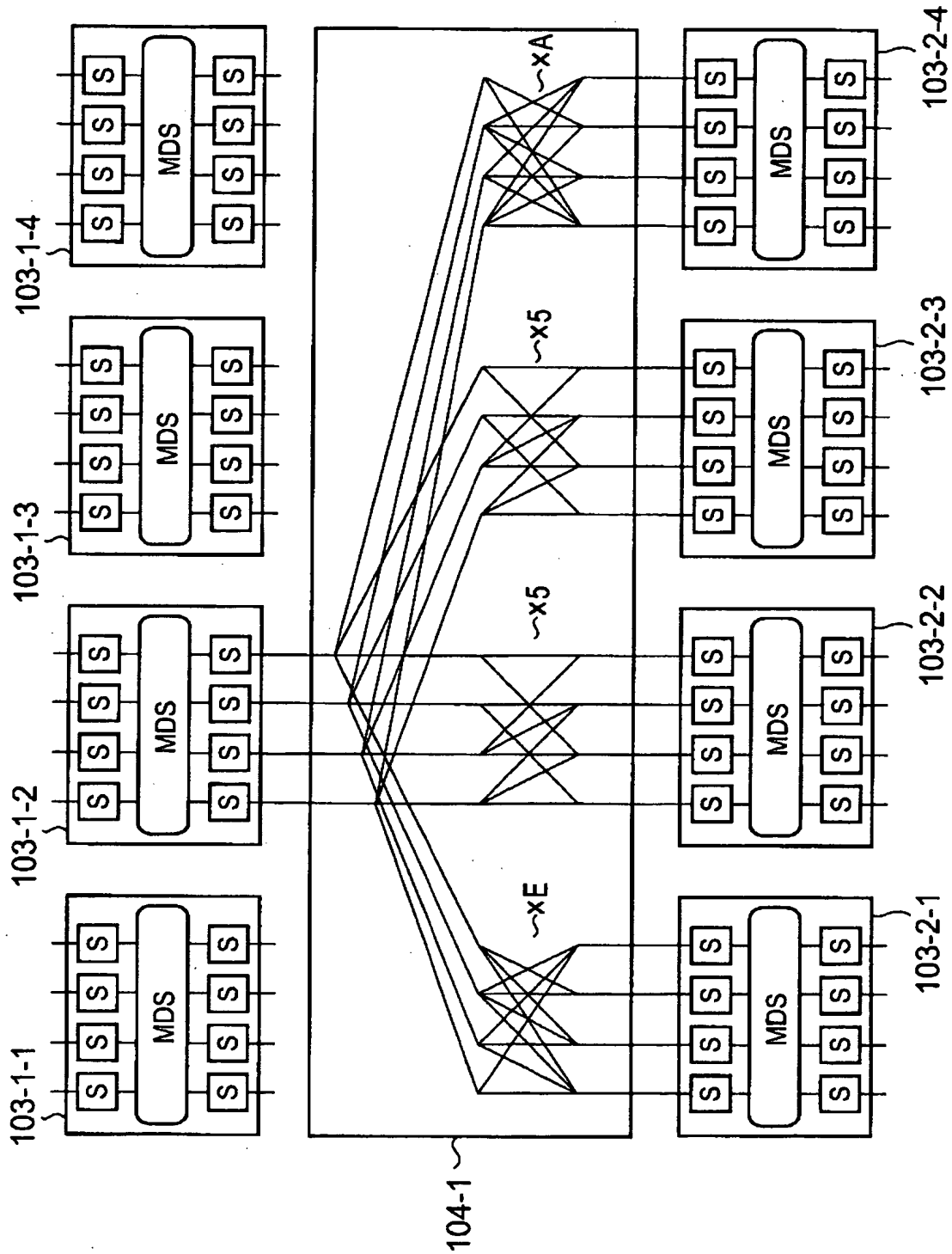
【図 2 9】



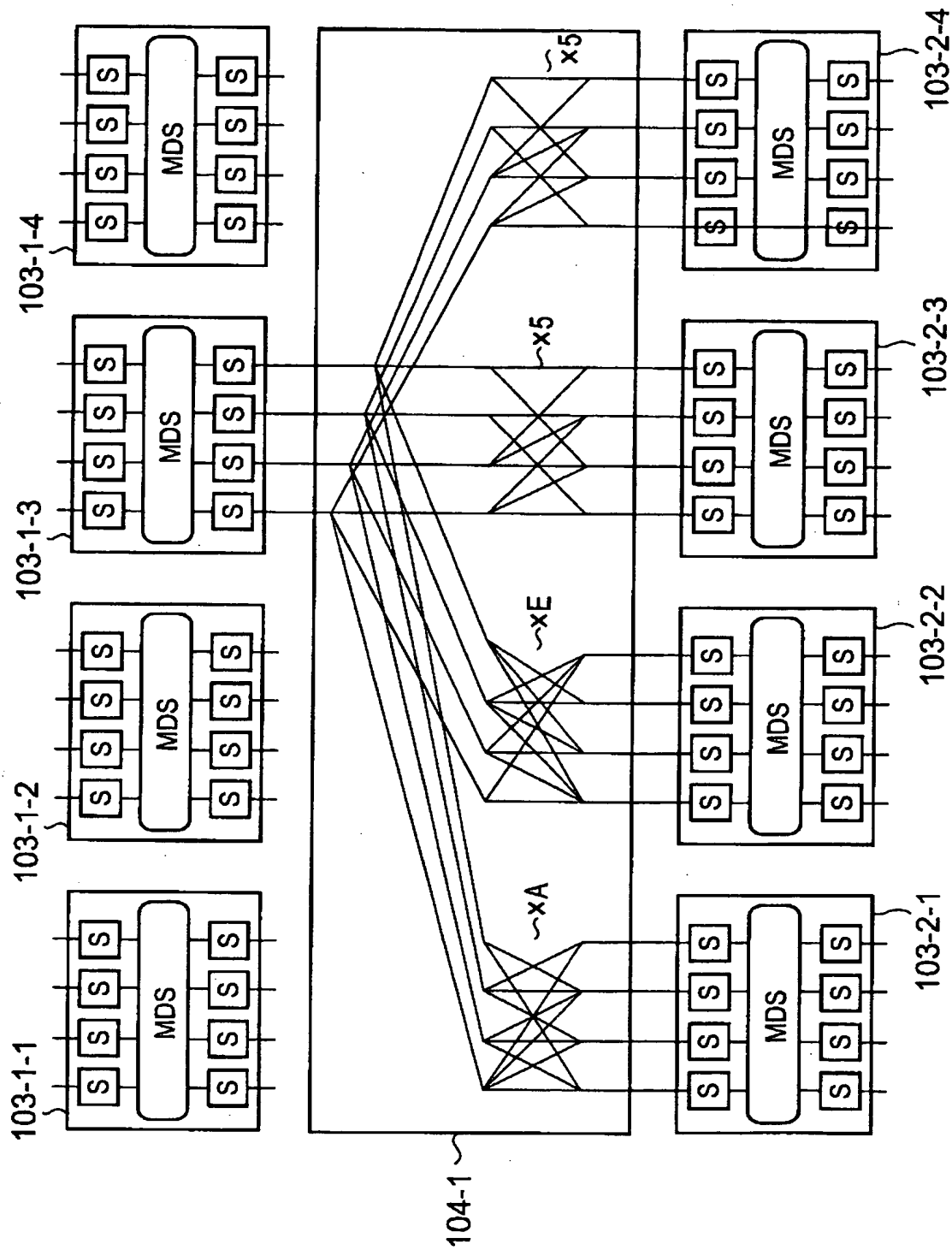
【図 30】



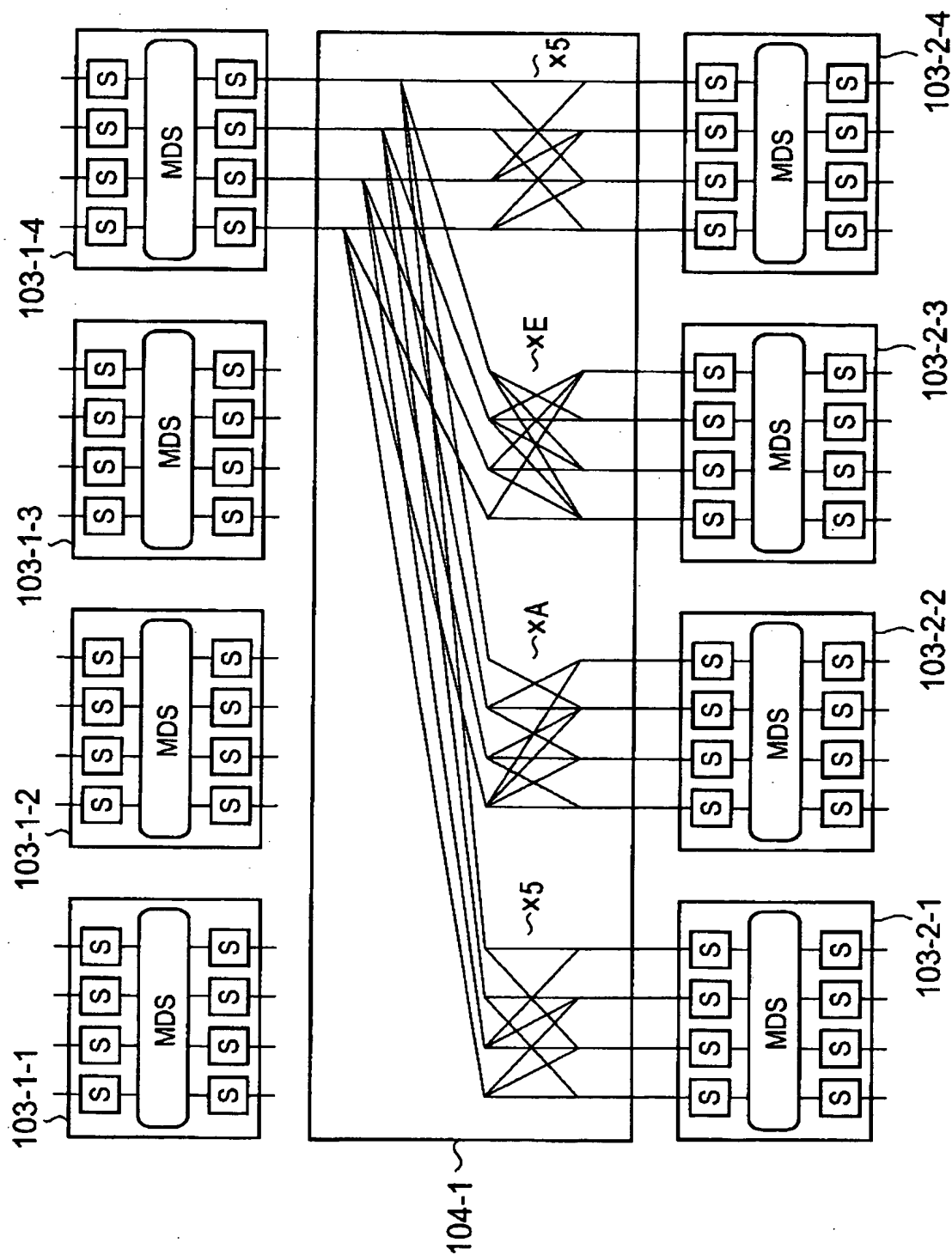
【図 31】



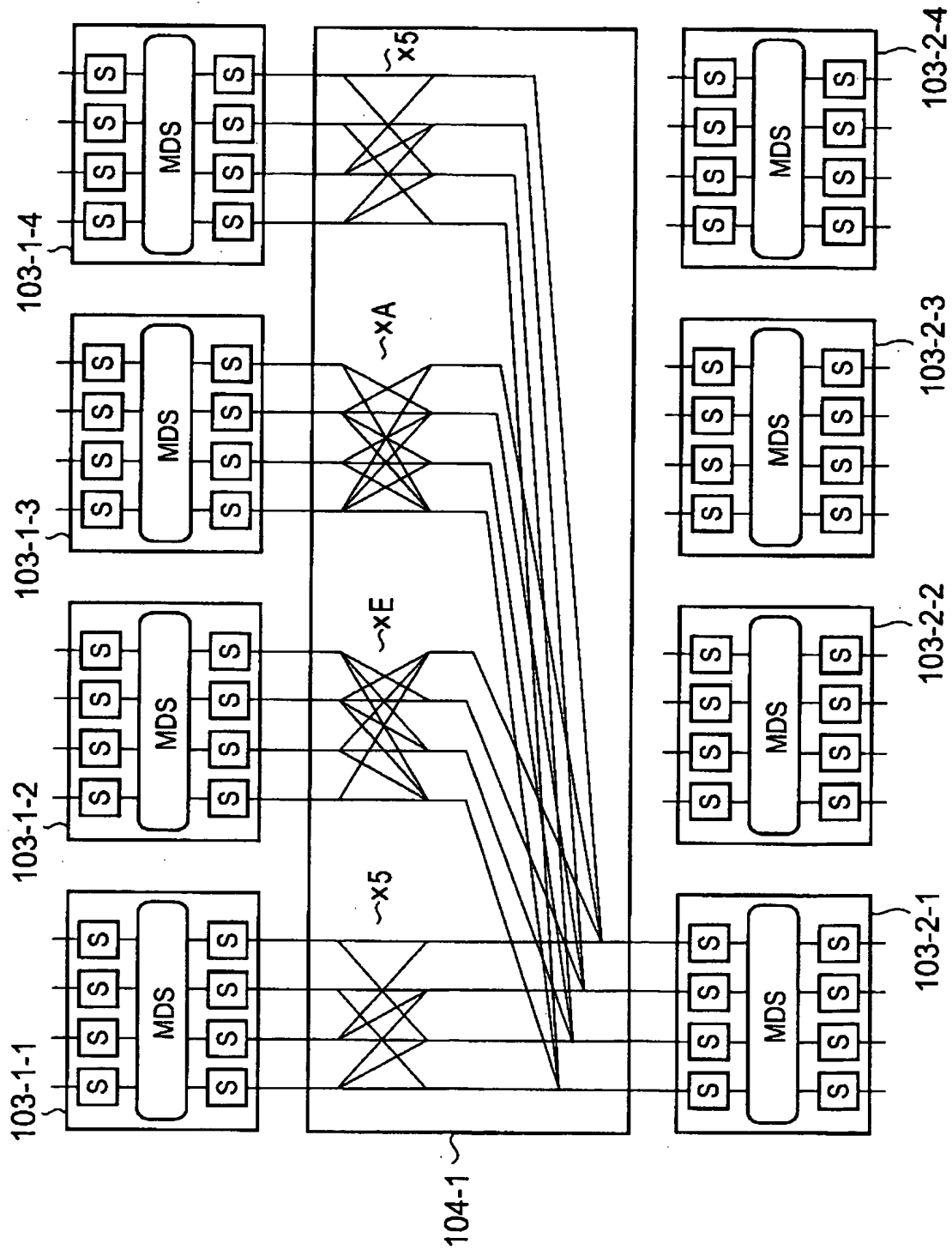
【図 32】



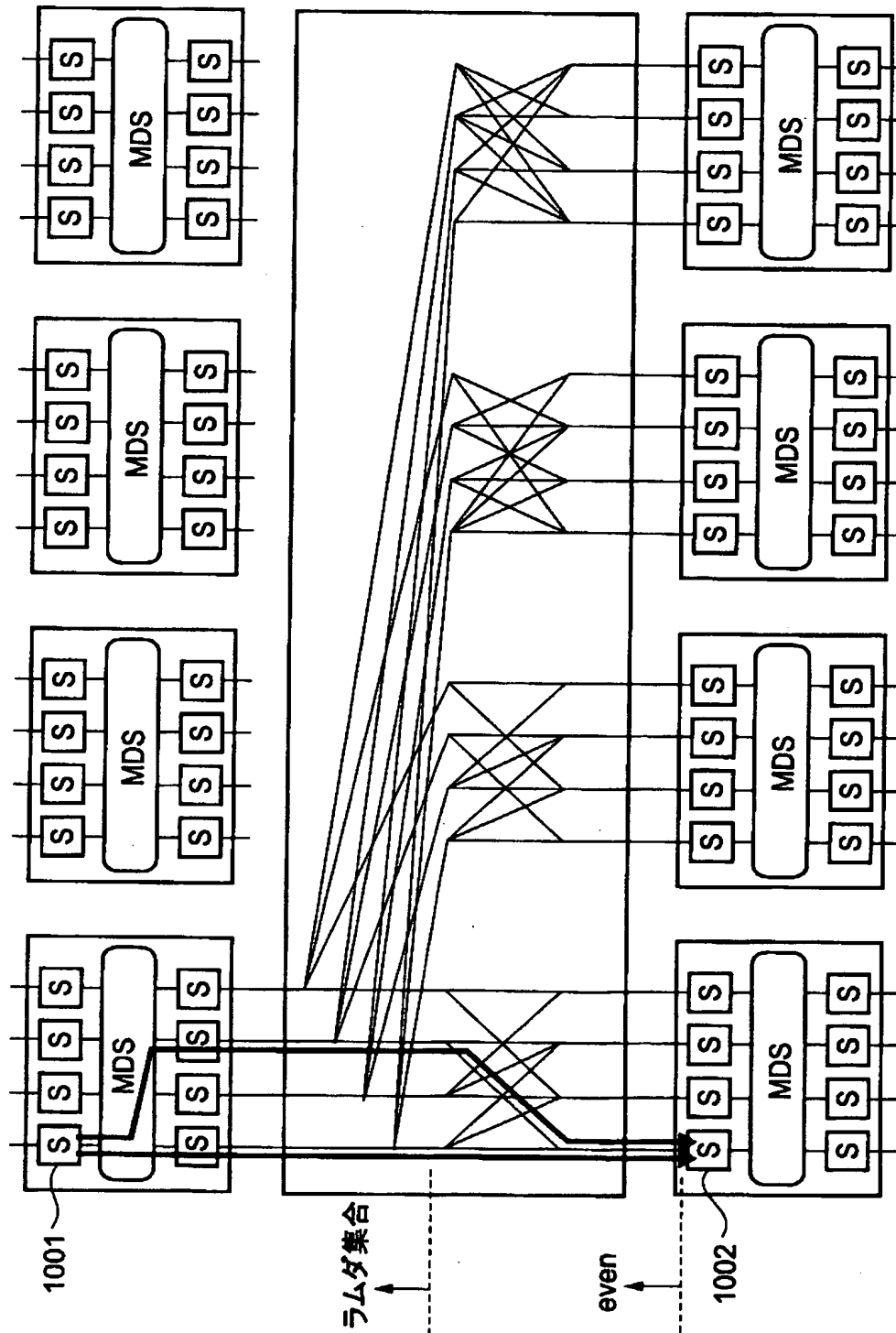
【図 33】



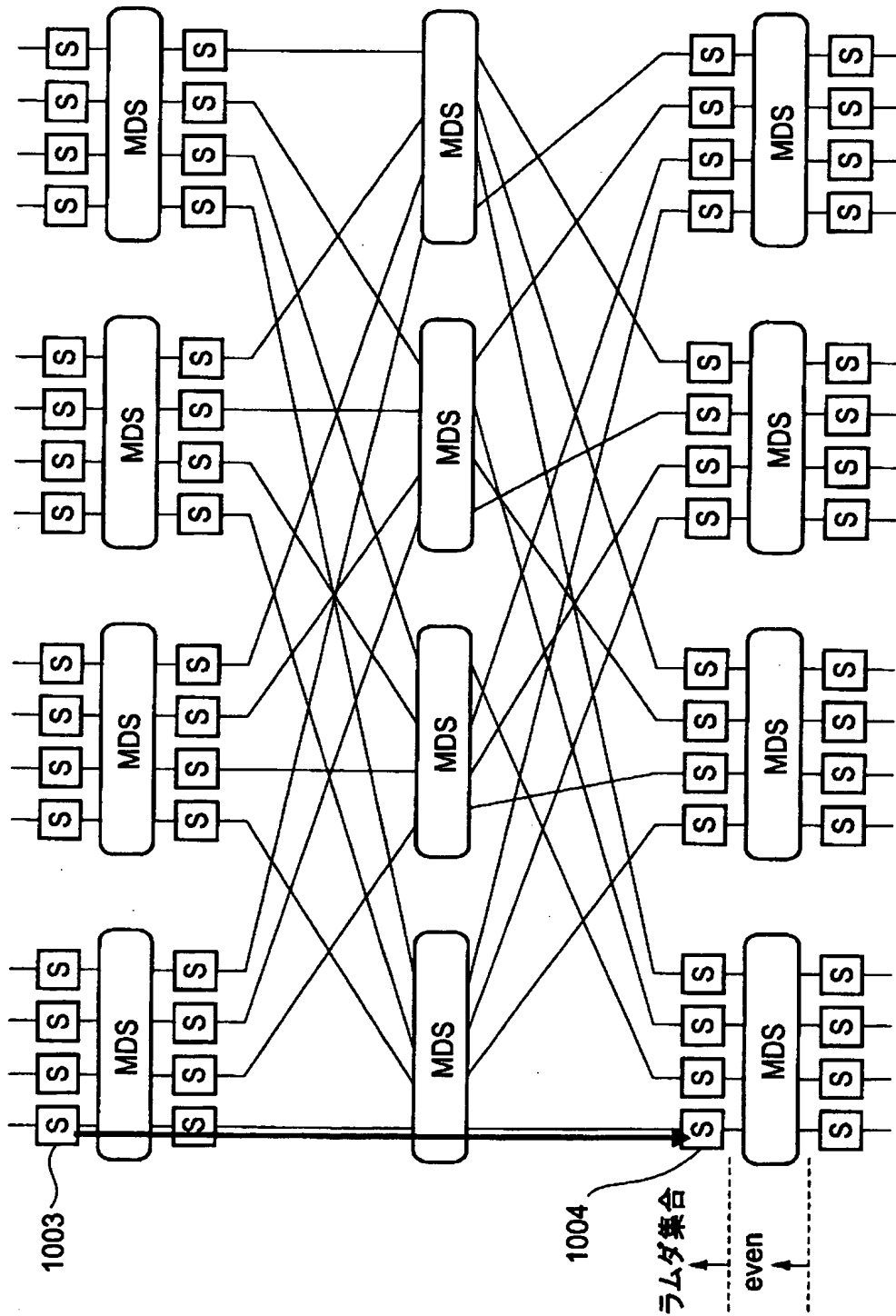
【図 34】



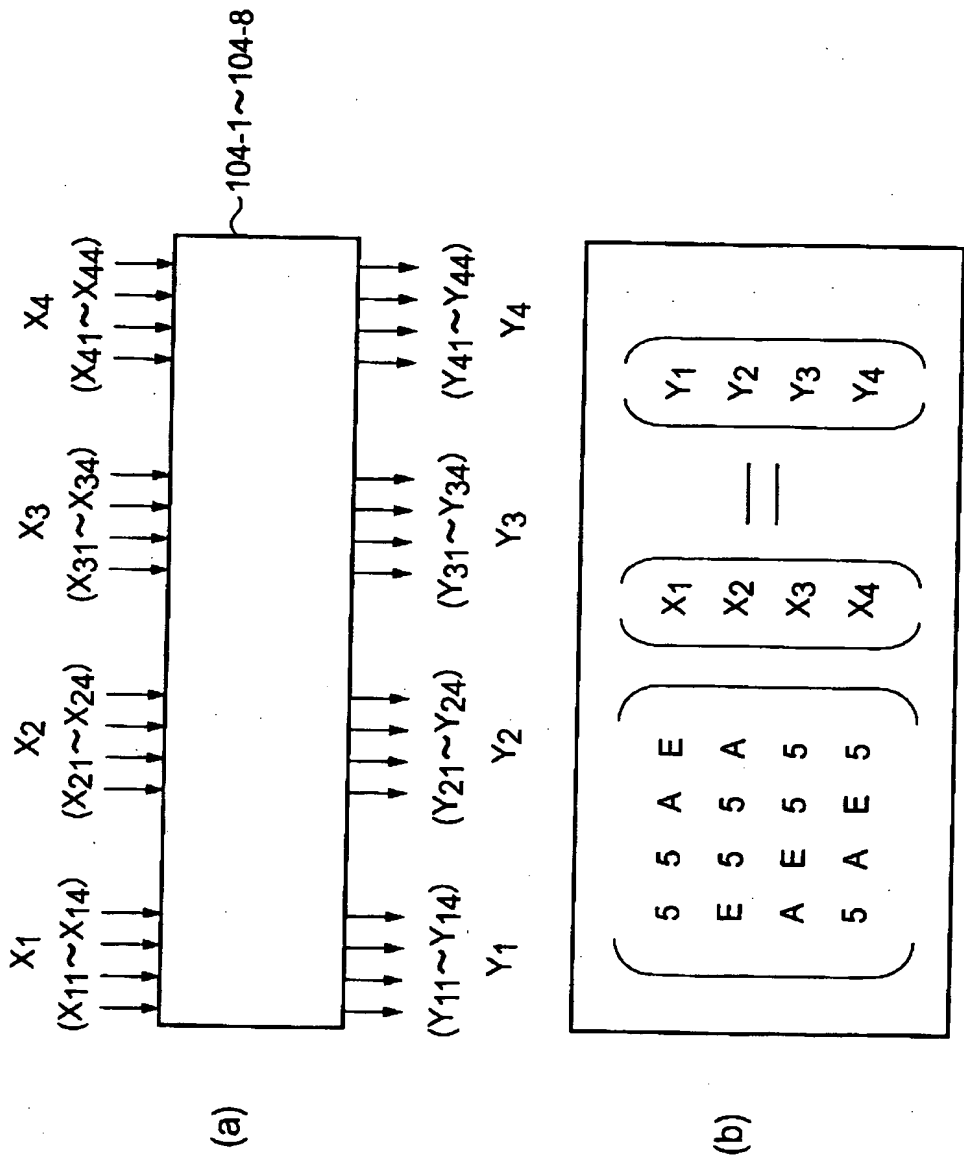
【図 35】



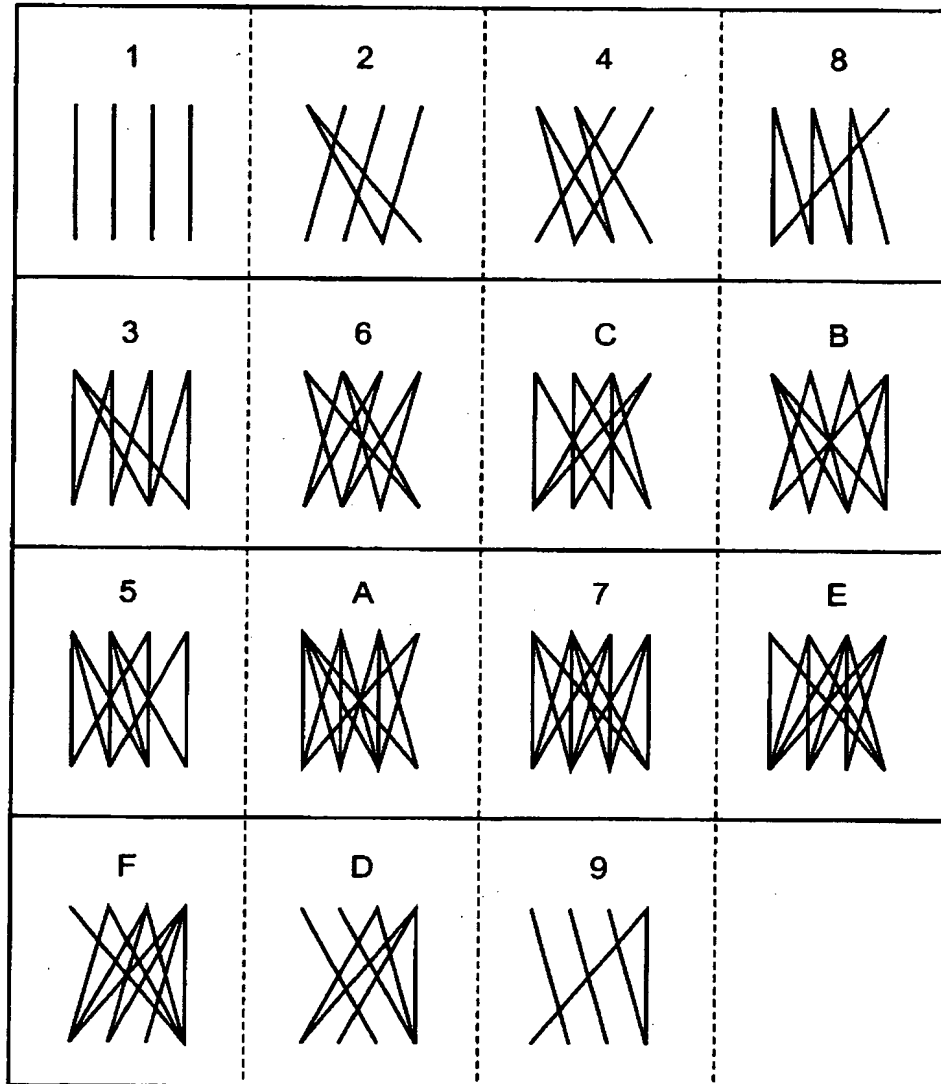
【図 36】



【図 37】



【図 38】



【図39】

$$(a) \begin{pmatrix} 5 & 5 & A & E \\ E & 5 & 5 & A \\ A & E & 5 & 5 \\ 5 & A & E & 5 \end{pmatrix} = M_1$$

$$(b) \begin{pmatrix} B & E & E & 6 \\ 6 & B & E & E \\ E & 6 & B & E \\ E & E & 6 & B \end{pmatrix} = M_2 = M_1^{-1}$$

$$(c) \begin{pmatrix} 6 & B & E & E \\ E & 6 & B & E \\ E & E & 6 & B \\ B & E & E & 6 \end{pmatrix} = M_3$$

$$(d) \begin{pmatrix} 5 & A & E & 5 \\ 5 & 5 & A & E \\ E & 5 & 5 & A \\ A & E & 5 & 5 \end{pmatrix} = M_4 = M_3^{-1}$$

【図40】

$$(a) \begin{pmatrix} 3 & 3 & 7 & C \\ C & 3 & 3 & 7 \\ 7 & C & 3 & 3 \\ 3 & 7 & C & 3 \end{pmatrix} = M_5$$

$$(b) \begin{pmatrix} B & E & 3 & 3 \\ 3 & B & E & 3 \\ 3 & 3 & B & E \\ E & 3 & 3 & B \end{pmatrix} = M_6 = M_5^{-1}$$

$$(c) \begin{pmatrix} 3 & 3 & B & E \\ E & 3 & 3 & B \\ B & E & 3 & 3 \\ 3 & B & E & 3 \end{pmatrix} = M_7$$

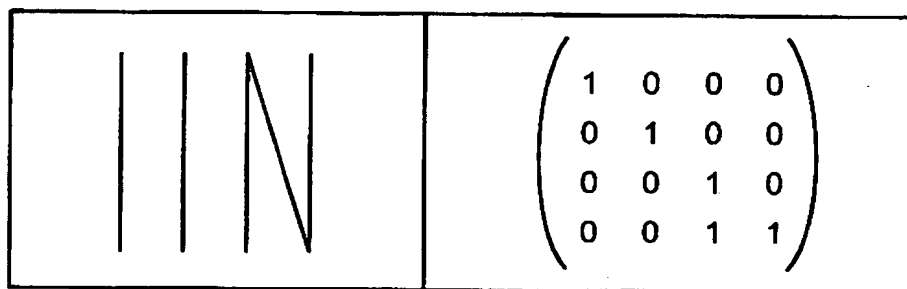
$$(d) \begin{pmatrix} 7 & C & 3 & 3 \\ 3 & 7 & C & 3 \\ 3 & 3 & 7 & C \\ C & 3 & 3 & 7 \end{pmatrix} = M_8 = M_7^{-1}$$

【図 4 1】

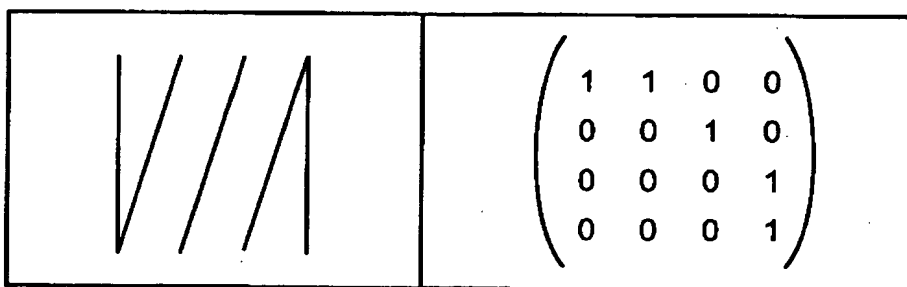
TABLE 1																															
CROSS-SECTIONAL DATA ON THE INCIDENCE OF TUBERCULOSIS IN THE UNITED STATES, 1946-1954																															
BY SEX, AGE, AND RACE																															
BY SEX, AGE, AND RACE (continued)																															
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	Y11	Y12	Y13	Y14	Y21	Y22	Y23	Y24	Y31	Y32	Y33	Y34	Y41	Y42	Y43	Y44
1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	X11	X12	X13	X14	X21	X22	X23	X24	X31	X32	X33	X34	X41	X42	X43	X44
1	1	1	0	1	1	0	1	1	1	0	1	1	1	0	1																
1	1	1	0	1	1	0	1	1	1	1	0	1	1	1	0																
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1																
1	1	1	1	1	1	0	1	0	1	0	1	0	1	0	1																
0	1	1	1	1	1	0	1	0	1	0	1	0	1	0	1																
1	1	1	0	1	1	0	1	0	1	0	1	0	1	0	1																
1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1																
1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1																
1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1																
1	0	1	0	1	1	1	1	1	1	0	1	1	1	1	1																
1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1																
1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1																
0	1	0	1	1	1	0	1	1	1	0	1	1	1	1	1																

【図 4 2】

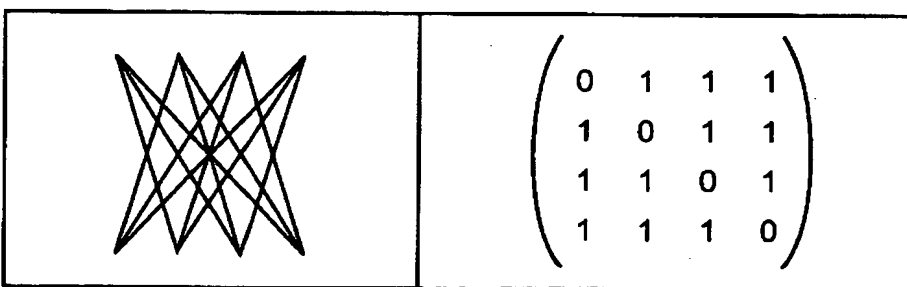
(a)



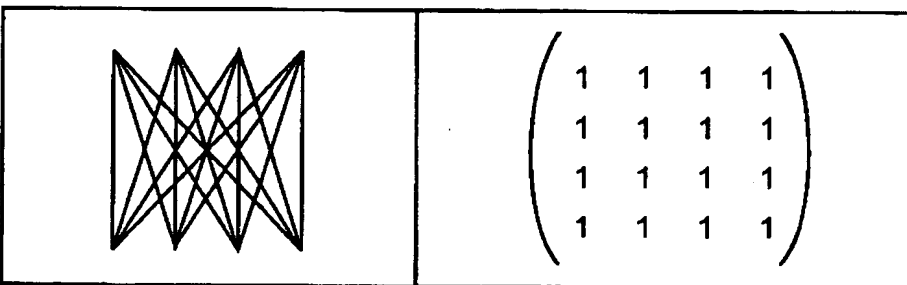
(a)



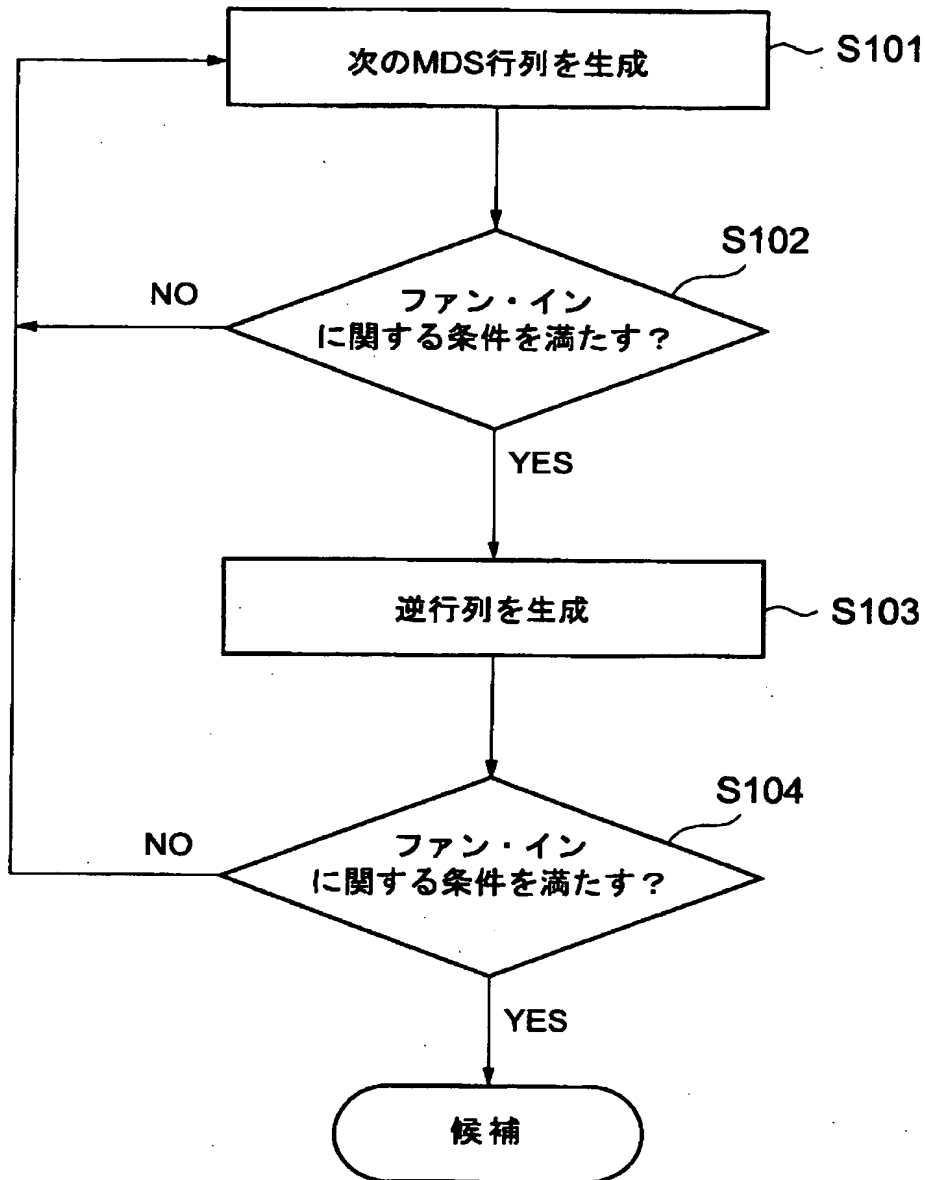
(a)



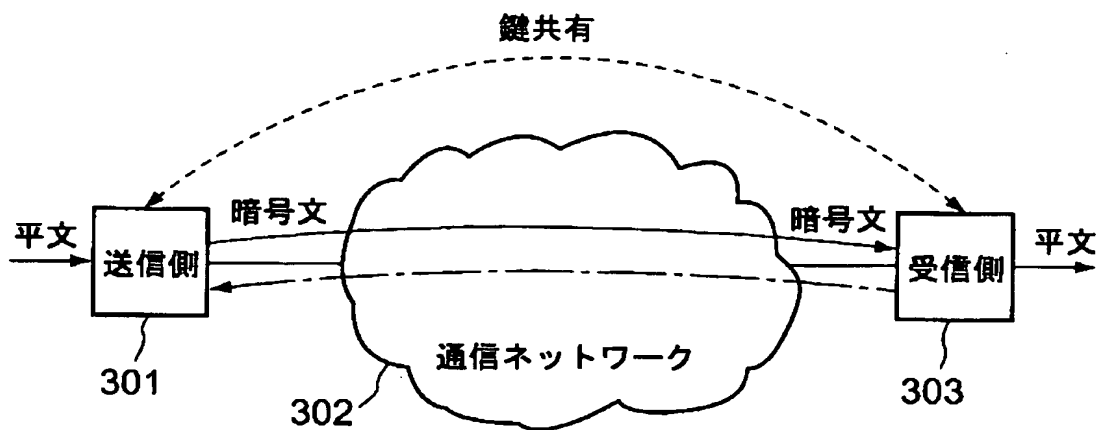
(a)



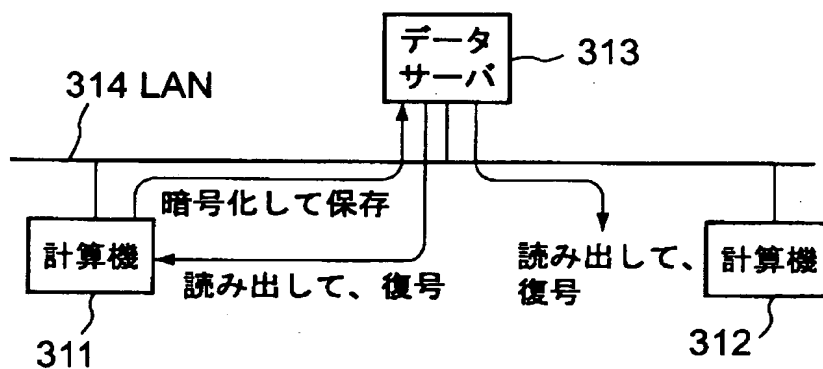
【図43】



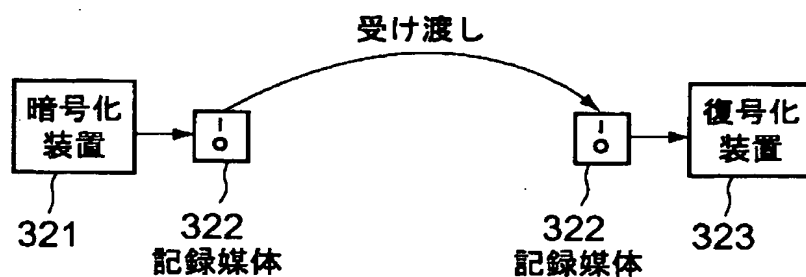
【図44】



【図45】



【図46】



【書類名】 要約書

【要約】

【課題】 計算コストを抑えたまま高く均一な拡散を可能とする暗号化装置を提供すること。

【解決手段】 各段において複数並列に並んだ非線形変換モジュール 2 の各々により局所的な小拡散を行い、次いで拡散モジュール 3 によりブロック幅に渡る大拡散を行い、また非線形変換モジュール 2 により局所的な小拡散を行い、ということを所定段数繰り返す。さらに、非線形変換モジュール 2 は、非線形変換モジュール 4 と拡散モジュール 5 とを交互に配列して構成される。すなわち、入れ子型 S P N 構造とする。拡散モジュール 3 は、前段の非線形変換モジュール群への入力データの少なくとも 1 つのビットの状態を後段の非線形変換モジュール群への入力データの少なくとも 1 つのビットへ複数の演算経路を辿って波及させるための線形変換を行う。

【選択図】 図 1

特2000-198478

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日 1990年 8月22日
[変更理由] 新規登録
住 所 神奈川県川崎市幸区堀川町72番地
氏 名 株式会社東芝